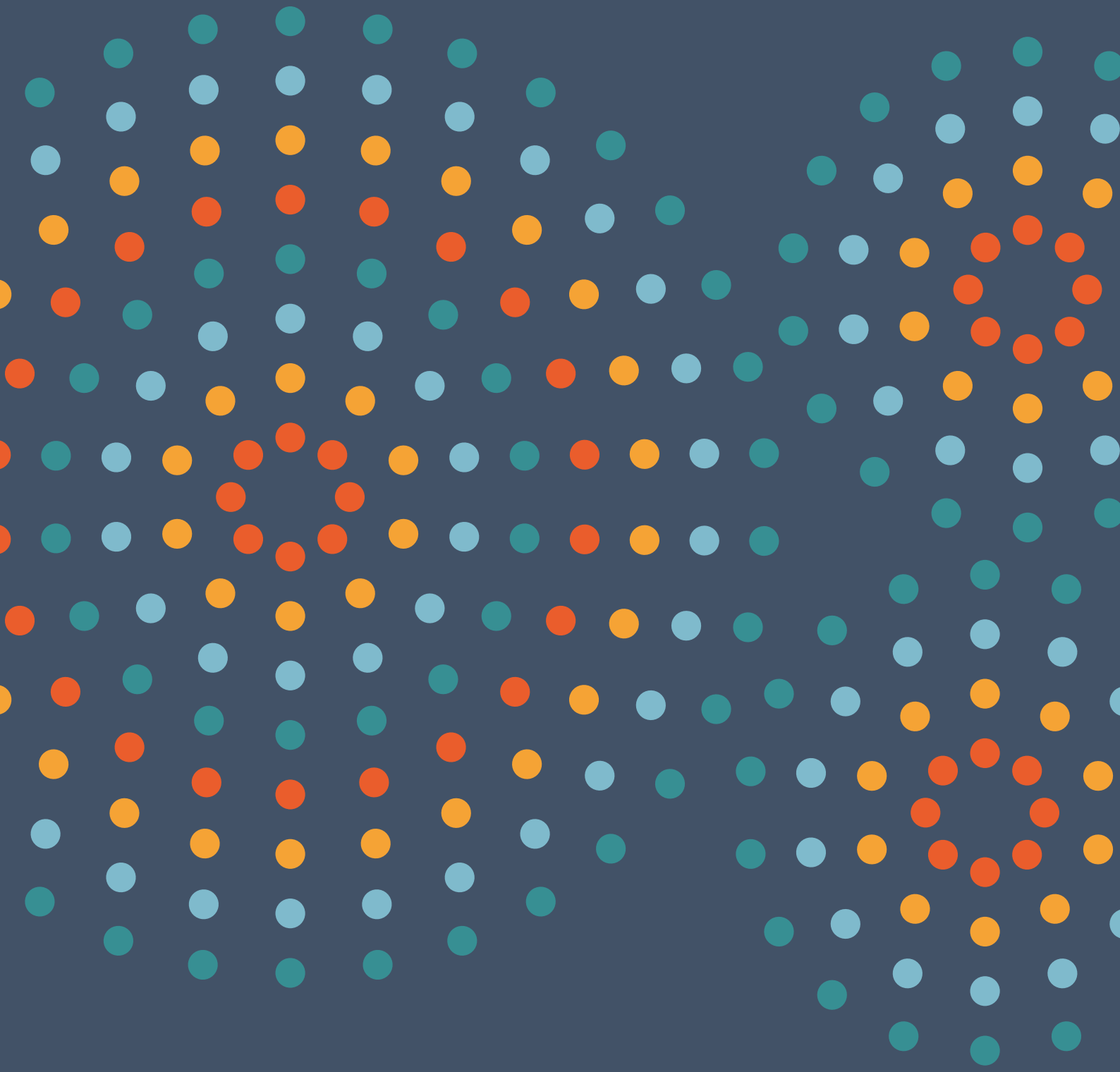
RegionalCooperationCouncil

Funded by
the European Union



Feasibility study for identification of technical interoperability in MONTENEGRO

good.better.regional.

Title:
Feasibility study for identification of technical interoperability in Montenegro

Publisher:
Regional Cooperation Council
Trg Bosne i Hercegovine 1/V, 71000 Sarajevo
Bosnia and Herzegovina
+387 33 561 700; Fax: +387 33 561 701
rcc@rcc.int
www.rcc.int

For publisher:
Regional Cooperation Council

Author:
Law and Internet Foundation

Coauthors:
Daliborka Spaić
Danilo Račić

Editor:
Tanja Maraš

Design:
Samir Dedić

July 2022

Table of Contents

Abbreviations

CAMSS	Common Assessment Method for Standards and Specifications
CENELEC	European Committee for Electrotechnical Standardisation
DEPIP	Data exchange protocol for interoperability and preservation
DESI	Digital Economy and Society Index
EBRD	European Bank for Reconstruction and Development
EC	European Commission
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and repealing Directive 1999/93/EC
eID	electronic identification
EIF	European Interoperability Framework
ENISA	European Union Agency for Cybersecurity
EU	European Union
GDP	Gross domestic product
IAF	International Accreditation Forum
ICT	Information and Communication Technologies
ISME	Institute for Standardisation of Montenegro
Law on Electronic Government	Law on eGovernment
LIF	Law and Internet Foundation
LS	Law on Standardisation of Montenegro
MAP REA	Multi-annual Action Plan for a Regional Economic Area
NGO	Non-governmental organisation
NIF	National Interoperability Framework
OECD	Organisation for Economic Co-operation and Development
OPP	Once-Only Principle
QTSPs/CTSPs	Qualified Trust Service Providers/Certified Trust Service Providers
QTS	Qualified Trust Services
RCC	Regional Cooperation Council
SDGR	Single Digital Gateway Regulation
SISEDE	Single Information System for Electronic Data Exchange
TBT	Technical Barriers to Trade Agreement

WB	Western Balkans economies (Albania, Bosnia and Herzegovina, Kosovo*, Montenegro, North Macedonia, Serbia)
WTO	World Trade Organisation

* This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence

I Executive Summary

The current report is divided into eight sections, which are providing an overview of the current state of play of Montenegro in terms of technical interoperability (particularly in the public sector with respect to trust services and electronic identification). In order to provide a comprehensive feasibility study, a brief overview of the economic situation and technical standards already in place has been presented, and some recommendations have been provided. For the purpose of compiling the report, a dedicated desk research has been carried out and an analysis of the existing relevant legal framework has been performed (though the team has encountered some difficulties due to the lack of English translations of some of the relevant legal acts). Furthermore, a tailored questionnaire has been elaborated and then filled by relevant experts, whose answers were carefully analysed and juxtaposed with the research findings. Thus, specific recommendations on the prioritisation and implementation of standards and specifications on technical interoperability have been provided, as well as clear guidelines in terms of the process of selection and adoption of standards and specifications, which will serve the planning of the upcoming steps towards complete technical interoperability of Montenegro's public authorities. To facilitate the cross-border/boundary provision of public services for Montenegrin authorities and citizens a list of minimum technical standards and specifications for enabling data exchange and document security for such cases has been mapped out.

Montenegro has achieved a certain level of interoperability readiness by adopting relevant legislative acts in the field. However, there is still some steps to be followed when it comes to the implementation of the existing legal framework. Thus, for Montenegro to achieve full digital interoperability of all central government and municipality bodies and their information systems, all administration information systems in Montenegro will need to connect with the Single Information System for Electronic Data Exchange (SISEDE). It is crucial to point out that there have been no technical barriers identified regarding such integration at the time of drafting this report. The results of the conducted analysis clearly demonstrated that Montenegrin authorities have the technical capacity to achieve such integration of SISEDE. However, allocation of additional resources is necessary as well as strong and continuous political will.

II Introduction

The following report analyses the level of technical interoperability in Montenegro, including the selected and adopted technical standards and specifications in the public administration information systems of Montenegro economy. The general purpose of the report is to support the Regional Cooperation Council (RCC) Secretariat in conducting a feasibility study, identifying the level of technical interoperability of public administration authorities in Montenegro and providing recommendations with respect to improving the level of technical interoperability. The overall goal of the feasibility study is to enhance the interoperability readiness of Montenegro with respect to trust services and electronic identification, boosting the creation of economy level accepted eID scheme and enabling cross-border/boundary provision of services.

The European Interoperability Framework (EIF) defines interoperability as "the ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems". One of the goals of the EIF is to provide guidance to public administrations on the design and update of national interoperability frameworks (NIF), or domestic policies, strategies and guidelines promoting interoperability.[1] This goal should be achieved through compliance of public administration information systems with the recommendations set out in the EIF, which will guarantee that NIFs adopted by the economies are developed in a coordinated and aligned way while providing the necessary flexibility to address specific requirements coming from domestic or domain-specific requirements.[2] Because of the necessary adjustments in line with the technological changes that occur, the applicable standards and changes in the environment in which business processes are implemented, Montenegro has adopted new National Interoperability Framework (NIF) in 2019. The NIF is based on the EIF and provides a set of recommendations to support public administration authorities in implementing interoperability activities.[3] With respect to technical interoperability, both the EIF and the NIF of Montenegro identify that one of the barriers towards achieving technical interoperability is the large number of inherited systems in the public administration, which lead to additional obstacles within the implementation of interoperable government services and fragmentation to a certain extent. In this regard, one of the recommendations provided in EIF and NIF is the use of formal and open standards and specifications, which will significantly enhance the level of technical interoperability.

1 European Interoperability Framework, page 5, available at: https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf, last accessed on: 24.11.2021

2 European Interoperability Framework, page 6, available at: https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf, last accessed on: 24.11.2021

3 Digital Public Administration Factsheet 2020 Montenegro, page 12, available at: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Montenegro_vFINAL.pdf, last accessed on 24.11.2021

In accordance with the eGovernment Benchmark Report 2021,[4] the overall eGovernment maturity of Montenegro economy is 37%, which is the lowest score from all the economies analysed in the report. The overall eGovernment maturity is measured on the basis of four indicators, namely: user centricity, transparency, key enablers and cross-border/boundary services.

However, in terms of recent efforts on digitalisation, Montenegro economy is one of the leading examples with 12 newly introduced online services between 2018 and 2020.[5] The Public Administration Strategy 2022 -2026 of Montenegro identifies achieving "Full interoperability of information systems and increasing the number of electronic services at a high level of sophistication" as one of the two operational objectives based on the challenges identified with respect to the ex officio exchange of data from official records, which is the legal obligation of the public authorities of Montenegro. As stated in the Strategy, the aim of the government is to harmonise all information systems so that they can be interoperable and to establish a full electronic exchange of data between registers, though the connection of all government and local authorities to the Single Information System for Electronic Data Exchange (SISEDE), also known as the Government Service Bus. With regard to addressing the abovementioned objective, the strategy prescribes a number of key performance indicators (KPIs), the fulfilling of which will serve as evidence for achieving the objective. For instance, the government of Montenegro aims to meet a few KPIs up until 2024, including to introduce 10 new digitalised services on SISEDE, increase the number of electronic exchanges between registers from the meta register to 30 (currently 8) and enhance the number of municipalities exchanging data through SISEDE to 10 (currently 1).

In accordance with Montenegro's Strategy for Information Society Development 2020, the technical and technological preconditions for transition to electronic operations within the public administration (e-government) are established through the implementation of two projects, namely - the e-government portal (web-services of the public administration) and eDMS (the electronic document management system within the public administration)[6]. In this regard, as stated above, the newly adopted Law on Electronic Government[7] has paved the way for Montenegro's transition to modern, paperless and efficient public administration.

The creation of interoperable public administration information systems and provision of e-services is regulated by the Law on Electronic Government (Zakon o elektronskoj upravi), adopted in the beginning of 2020. In accordance with Art. 3 of the latter, "electronic administration functions through a unique information system of bodies, information and communication network of bodies and electronic data exchange systems, as well as through information systems by bodies and their entities." The Law is considered to be crucial for boosting the provision of e-services by public authorities and enhancing the provision of

4 eGovernment Benchmark Report 2021, available at: https://www.capgemini.com/wp-content/uploads/2021/10/eGovernment-Benchmark-2021-Insight-Report.pdf, last accessed on 24.11.2021

5 eGovernment Benchmark Report 2021, page 25, available at: https://www.capgemini.com/wp-content/uploads/2021/10/eGovernment-Benchmark-2021-Insight-Report.pdf , last accessed on 24.11.2021

6 Strategy for the Information Society Development 2020, page 70, available at: https://www.gov.me/en/documents/68736414-503b-41bb-81b0-753b581fb386

7 Available at: https://www.gov.me/en/documents/0ee38c03-d492-462c-937b-f2a029bc58ad

e-services to both citizens and business, as it introduces the Single Information System for Electronic Data Exchange (SISEDE) and prescribes the rules for its use and management, including the exchange of information between bodies with regard to the provision of electronic administrative services. According to the European Interoperability Framework Monitoring Mechanism 2019, the level of technical interoperability in Montenegro is as high as the average level in all EU Member States.[8] However, the identified level of organisational interoperability and interoperability governance is considered to be middle-lower.

8 Available at: https://joinup.ec.europa.eu/collection/national-interoperability-framework-observatory/2019-eif-monitoring-mechanism

III Methodology

The current report has been elaborated following a well-established methodology, which takes into account the current state of play of Montenegrin economy, its political context, legal framework and overall societal digital development. The findings are based on complex methodology combining various research techniques. Each of them aims to tackle a particular issue in the best possible way. Thus, to ensure complementarity from methodological perspective several different approaches have been employed in order to provide a comprehensive overview:

1. Desk-based research

It aims to provide an overview (including macroeconomic) of Montenegro with respect to the level of technical interoperability, particularly in the provision of public services. The research will identify the current status quo of the economy and thus, it will set up the context for further elaboration of the feasibility study. The approach includes a review of available studies, analyses, strategic documents, reports and recommendations relevant for eID, trust services and enhancing the level of technical interoperability. Once the criteria laying the foundation of the assessment have been put in place, the team of experts has proceeded with collecting relevant information. For this purpose, sources such as reports by European Commission, ENISA, UN, World Bank, OECD, etc. have been used. Where deemed necessary, further investigation has been pursued regarding selected topics.

2. Legal analysis

The legal analysis conducted within the scope of the feasibility study represents an analysis comprising a variety of different laws and bylaws in the sphere of eID and trust services, especially regarding the technical standards and specifications which should be met by the administration systems. Some of the identified legal acts were acquired within the desk-based research, while others were provided by representatives of the Ministry of Public Administration upon enquiry made by Law and Internet Foundation. The legal analysis has been focused on the identification of technical standards and specification, which have already been prescribed as mandatory by laws and/or bylaws, so that they could be compared with the prescribed standards and specifications in accordance with the best practices within the EU, providing a list of those which should be implemented. It should be noted that the individual legal acts acquired through both ways are not legally translated documents, which hampered the analysis of the framework to a certain extent.

3. Expert questionnaire

An expert questionnaire has been designed with the aim to compile in-depth information on a domestic level regarding the technical interoperability of the respective domestic systems taking into account the EU technical interoperability framework to ensure integrated public service delivery. The respective questionnaire has been distributed to representatives of the Ministry of Public Administration, and has been filled by their respective experts. The questionnaire is quite thorough and outlines the standards which need to be implemented with respect to the electronic identification, trust services and provision of e-services (e- signatures, e-seals, e-time stamps, e-delivery, website authentication, e-documents, etc.). The questionnaire is structured in a way not only to reflect the consistency with the standards prescribed in EU level, but also to require the respondent to elaborate on the nature of the identified inconsistency, thus allowing LIF team to formulate relevant recommendations. In particular, the representatives of the Ministry were asked to provide details of the identified standards in place as well as deviations of the legislation where no complete harmonisation of the domestic legislation with the EU acquis is noted. The questions included in the questionnaire represent a baseline for the assessment, meaning that responding to them is mandatory so comprehensive data on the respective economy is gathered. However, the correspondents were, of course, allowed to expand on any topic which is of particular interest to the assessment exercise. This means that some subjects can be covered more extensively than others. An example of the questionnaire is available to the current report as Appendix I.

4. Framework analysis

The analysis has been made based on the completed questionnaire, enriched by the findings of the desk-based research and verified by the follow-up call with experts from the respective Ministry. The purpose of the analysis of the questionnaire is to indicate both the relevant steps that should be followed and the technical standards which shall be adopted in order for the level of technical interoperability to be enhanced.

IV Overview of Montenegro's economic situation and level of technical interoperability in the public sector with respect to trust services and electronic identification

Only two years after proclaiming its independence (2006) Montenegro submitted its application to join the European Union (EU) in 2008. Four years later (2012) the negotiations have been initiated by the European Commission (EC).[9] The status of Montenegro in terms of the EU is still 'candidate country'. The report notes that there is still much to do in terms of the rule of law. Therefore, improvements in that area will be key for any further progress of the negotiation between the EU and Montenegro. The improvement in terms of digital governance, related services and interoperability between various systems would be an essential part of it taking into account the ongoing technological advancements.

1. Analysis of the current economic situation in Montenegro

1.1 Market analysis

Montenegro's economy is highly dependent on tourism (part of the service sector).[10] So the COVID-19 pandemic has had a huge negative impact on the economy's current situation, which reflects on the employment rates, investments, public and private finances as well as the trade level.[11] In addition, there is a long pending reform in terms of Montenegro's public administration which for sure will affect the interoperability level of the economy. In addition, the level of readiness of Montenegro in terms of implementing the EU acquis is considered insufficient.[12] Despite the pandemic and its spill-over effect, the government has managed

9 COMMISSION STAFF WORKING DOCUMENT Montenegro 2021 Report Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2021 Communication on EU Enlargement Policy SWD/2021/293 final. Available at: https://ec.europa.eu/neighbourhood-enlargement/enlargement-policy/negotiations-status/montenegro_en. Last accessed 19/11/2021.

10 COMMISSION STAFF WORKING DOCUMENT Montenegro 2021 Report Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2021 Communication on EU Enlargement Policy SWD/2021/293 final. Available at: https://ec.europa.eu/neighbourhood-enlargement/montenegro-report-2021_en, last accessed 24/11/2021.

11 Available at: https://ec.europa.eu/neighbourhood-enlargement/montenegro-report-2021_en, last accessed 24/11/2021.

12 Ibid.

to keep up with the plan for developing the business environment by implementing certain reforms (e.g. minimise the fiscal risks). Thus, the overall financial situation has been currently assessed as 'stable'.[13] However, the pandemic has exacerbated Montenegro's need to diversify itself in terms of sectors and industry branches. The major barriers identified are the insufficient innovation capacities, quality and inability of education to address the discrepancies between existing and required skills' sets, lack of adequate transport infrastructure, tiny local companies and the fact that they almost do not compete in markets outside Montenegro. However, it is worth noting that there is an increase in the deployment of novel telecommunication and energy infrastructure.[14] Moreover, EU standards have been applied to local companies as well as some legislative prerequisites have been introduced in terms of electronic registration of companies. To ensure better competitiveness within the EU market, Montenegro's economy needs diversification.

Some of the key statistics for the economy are the following:[15]

Population: 622 182	**Area: 13 812 km²**
Capital city: Podgorica	Official language: Montenegrin
Currency: Euro	EU member status: No, candidate status
Average gross salary: 798 EUR[16]	GDP: 4.3 GDP per capita: 6 900

1.2 Geo-political analysis

Montenegro is NATO member since 2017.[17] It is one of the three Western Balkan economies which is part of the alliance, which makes it clearly a key geo-political factor not only within the region. As already mentioned above Montenegro has been a candidate for joining the EU for more than 10 years now. Thus, their technical interoperability readiness will be a key factor on the road towards complete EU integration.

1.3 Digitalisation analysis

Digitalisation is an inevitable process, which has become such due to globalisation trends and the constantly developing technologies. Montenegro has initiated a public administration reform (2022-2026) and its structure, though there have been some delays in terms of its finalisation. However, there are some achievements and one of them is the push for electronic government and the opened public dialogue regarding legislative changes in the Law on

13 Available at: https://ec.europa.eu/neighbourhood-enlargement/montenegro-report-2021_en, last accessed 24/11/2021.
14 Available at: https://ec.europa.eu/neighbourhood-enlargement/montenegro-report-2021_en, last accessed 24/11/2021.
15 Available at: https://ec.europa.eu/eurostat/documents/3217494/9799207/KS-GO-19-001-EN-N.pdf/e8fbd16c-c342-41f7-aaed-6ca38e6f709e?t=1558529555000, last access 19/11/2021.
16 MONSTAT, STATISTICAL OFFICE OF MONTENEGRO, 'Average earnings (wages) October 2021', available at: http://www.monstat.org/eng/novosti.php?id=3413, last accessed 02/12/2021.
17 'Montenegro joins NATO as 29th Ally' (June 9, 2017), available at: https://www.nato.int/cps/en/natohq/news_144647.htm, last accessed 02/12/2021.

Access to Information.[18] Both of these initiatives will play a key role in terms of interoperability readiness. The latter will facilitate access to information by the general public while the former will provide efficient access to electronic public services and others.[19]

There is still a lot to be achieved in terms of legislative amendments, optimisation of public administration and strong political will, which will facilitate a high level of interoperability (including technical one) as well as better accountability. A noteworthy development is the recently set up register of institutions and government bodies by the Ministry of Public Administration. In addition, the Council for electronic government has been set up in accordance with the existing Law on Electronic Government, which will potentially improve the practical application of that legislative act and its secondary acts. [20] Few changes have been adopted in terms of the Law on Electronic Identification and Electronic Signature. One of the outcomes is the recently introduced Register of qualified providers of electronic trust services and the very fact that citizens (based on the Law on Identity Card ("Official Gazette of Montenegro", No. 12/2007, 73/2010, 28/2011, 50/2012, 10/2014 and 18/2019) from June 2020), through the use of a new ID card, can use the certificate for qualified electronic signature and the certificate for electronic identification completely free of charge while for businesses the cost is relatively low.[21] This, undoubtedly, fosters the wider usage of electronic services across the economy and abroad. In accordance with the Law on Electronic Identification and Electronic Signature, the Ministry of Public Administration is obliged to maintain and publish on its website the following:

- Register of qualified providers of electronic trust services (Post Office of Montenegro, CoreIT doo, Ministry of the Interior, Montenegrin Telekom Podgorica);
- Records of providers of electronic trust services (Post Office of Montenegro, CoreIT doo, Montenegrin Telekom Podgorica, Zeko.ME doo, CBCG - Central Bank of Montenegro, Ministry of Public Administration).

For the needs of public administration bodies, certificates for advanced electronic signatures are issued by the Ministry of Public Administration. Here it should be duly noted that the Ministry of Interior is the only issuer of electronic identification means with a high level of assurance. New ID cards with eID are being issued since June 2020. National ID card contains a chip with an identification certificate and a certificate for a qualified electronic signature. In accordance with the Law on Personal Identification Card, all citizens in Montenegro will have a new ID card as of June 2025. A major disadvantage is the pace of deploying most of the public services, including the digital ones, and the overall lack of efficiency in terms of their practical usability (e.g. time effectiveness, not user friendly). For instance, the Single Information System for Electronic Data Exchange (a.k.a. Government Service Bus platform), which is supposed to facilitate the exchange of data and thus improve the interoperability level,

18 Available at: https://ec.europa.eu/neighbourhood-enlargement/montenegro-report-2021_en, last accessed 24/11/2021.
19 Available at: https://ec.europa.eu/neighbourhood-enlargement/montenegro-report-2021_en, last accessed 24/11/2021.
20 Available at: https://ec.europa.eu/neighbourhood-enlargement/montenegro-report-2021_en, last accessed 24/11/2021
21 Ibid.

is still not functioning properly according to its full capacity. Therefore, the overall provision of public (including digital) services is rather limited in Montenegro.

The newly introduced Law (in June 2020) regarding electronic ID cards provides for e-identification and e-signature, which will ease and encourage citizens to use digital public services. However, the operational capacity of the available electronic services (e.g. electronic payments) is limited despite their formally increased number.[22] Another relevant legislative act has been enforced, namely the Law on Electronic Government (eGovernment), which aims to enable citizens and businesses' access to public administrative services.[23] At the same time, this legal document intends to push for the wider and coordinated deployment of technologies (information and communication) within the public administration and their provision of services. Thus, the Law on eGovernment is the main legislation regulating the interoperability in Montenegro along with the Council established under its framework and the respective bylaws.[24] There are others, recently adopted legal acts, regulations and rulebooks, which aim to facilitate the interoperability in the economy and thus improve its overall functioning by providing its citizens and business entities with a wide variety of electronic public services. For instance, the following ones:[25]

- The Electronic Document Act (regarding the use of e-documents and the rights of involved parties);
- Regulation on Data Management Content and Method in a Single Information System for Electronic Data Exchange;
- Regulation on the Mode of Work, Content and Management by the eGovernment Portal;
- Rulebook on the Management and Functioning of the Document Management Information System (eDMS);
- Law on Electronic Identification and Electronic Signature;
- Rulebook on eID and Rulebook on Open Data;
- Law on Information Security;
- Law on Personal Data Protection;
- Regulation on Information Security Measures;
- Law on Services (prescribes the legal ways to establish and regulate the exchange of information with EEA countries).

22 Available at: https://ec.europa.eu/neighbourhood-enlargement/montenegro-report-2021_en, last accessed 24/11/2021
23 Digital Public Administration factsheet 2020, Montenegro, Available at: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Montenegro_vFINAL.pdf, last accessed 01/12/2021.
24 Digital Public Administration factsheet 2020, Montenegro, Available at: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Montenegro_vFINAL.pdf, last accessed 01/12/2021.
25 Digital Public Administration factsheet 2020, Montenegro, Available at: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Montenegro_vFINAL.pdf, last accessed 01/12/2021.

2. Technical standards in use and planned to be used in the public administration information systems

2.1 List of identified public administration authorities

The following list of public administration authorities includes 18 ministries and 24 administrative bodies in Montenegro:

Public Administration Authorities of Montenegro	
Public authority	**Competence**
Ministries	
Ministry of Justice	Administration of justice, management and organisation of the judiciary, international judicial cooperation administration regarding penalties and criminal sanctions;
Ministry of the Interior	Administration of public security, emergency management and civil protection, civil registration and identification, refugees and borders;
Ministry of Foreign Affairs	Representation of Montenegro in relations with other countries, international organizations and other international institutions, preparation of draft laws, other regulations and general acts in the field of foreign affairs, giving opinions on draft laws and other regulations regulating issues related to foreign affairs; carrying out work in accordance with the law governing the conclusion and execution of international agreements and other regulations or international agreements;
Ministry of Defence	Defence policy and international cooperation in defence and security;
Ministry of Finance	Economic, fiscal and social policies, administration of state aid and public procurement;
Ministry of European Affairs	Foreign policy, international representation and cooperation, diplomatic and consular affairs; management and coordination of the process of stabilization and association and accession of Montenegro to the European Union in the part related to monitoring the implementation of the Stabilization and Association Agreement between the European Communities and their member states on the one hand and Montenegro on the other
Ministry of Public Administration	Public administration policies, implementation of digitalisation, information security, e-government and interoperability;
Ministry of Education	Management of the educational system, organisation of scientific research, protection and preservation of cultural goods, development of sport;

Public Administration Authorities of Montenegro	
Public authority	**Competence**
Ministry of Culture and Media	Development of cultural and artistic creativity; protection, preservation, valorization and presentation of cultural heritage; development of creative industries; realization of public interest in culture; preparation of draft laws, other regulations and general acts in the field of culture, giving opinions on draft laws and other regulations regulating issues related to culture; development and implementation of cultural development strategies and programs; research in culture;
Ministry of Science and Technological Development	Implementation of programs of general interest that involve scientific research institutions and researchers in the European Research Area and international scientific and innovative programs; development of plans and programs of scientific research activities; development of scientific research policy and strategies; preparation of draft laws, other regulations and general acts in the field of science and research;
Ministry of Sports and Youth	Preparation of draft laws, other regulations and general acts in the field of sports and youth; monitoring and determining the situation in the field of sports; preparation of development strategies and other measures used to create policies in the field of elite, recreational, children's, school and university sports; improvement and implementation of the Sports Development Strategy;
Ministry of Human and Minority Rights	Protection of human rights and freedoms, if this protection is not within the competence of other ministries; protection against discrimination; monitoring the realization and protection of the rights of members of minority nations and other minority national communities in terms of national, ethnic, cultural, linguistic and religious identity; improvement of mutual relations between members of minority nations and other minority national communities; improvement of inter-ethnic tolerance in Montenegro,
Ministry of Labour and Social Welfare	Preparation of regulations in the field of labor relations, protection and health at work; labor and employment markets; wages and other incomes from and on the basis of work, preparation of regulations in the field of social and child protection, pension and disability insurance, veterans and disability protection; financial aid to a foreigner seeking international protection and an asylum seeker and a foreigner under subsidiary protection; family protection;
Ministry of Health	Health policy, management of health care and insurance systems and public health;
Ministry of Economic Development and Tourism	Regional development, competitiveness, labour and tourism policies with administrative tasks in relation to business, trade, consumer protection, competition, standardisation, concessions, intellectual property, internet, telecommunications and postal services;

Public Administration Authorities of Montenegro	
Public authority	**Competence**
Ministry of Agriculture, Forestry and Water Management	Agricultural, rural development and water management policies and administrative tasks in veterinary, food safety, fisheries, forestry and land management, wildlife sectors;
Ministry Ecology, Spatial Planning and Urbanism	Environmental protection, housing and climate policies and administrative tasks in natural resource management, waste management, utilities, spatial planning and construction sector;
Ministry of Capital Investments	Regulation and investment preparation in maritime, road, sea, rail and air transport and natural resource exploitation, concessions in energy and mining;
Administrative Bodies	
Institute for the Execution of Criminal Sanctions	Execution of criminal sanctions;
National Security Authority	Classified information protection, standardisation, and regulation;
Revenue and Customs Administration	Tax and levies collection, register maintenance, regulation of games of chance, customs control and intellectual property protection;
Cadastre and State Property Administration	Cadastre and land survey, register-keeping on property and management of public property;
Statistical Office	Collection and processing of statistical data and statistical analysis and research;
Institute for Social and Child Protection	Supervision, research and advising in the areas of social policy and child protection, supervision of social and child protection services;
Department for Diaspora and Emigrants	Cooperation with and support of Montenegrin diaspora;
Human Resources Management Authority	Human resource services for staff administration and civil servants;
Bureau for Education Services	Quality control in educational system, research, advising and development in educational policy;
Administration for Protection of Cultural Property	Research, study, documentation and recording of cultural heritage, cultural property protection and conservation;
State Archive	Research, collection and upkeep of public and private archives;
Bureau of Metrology	Application of metrology standards in Montenegro;
Directorate for Food Safety, Veterinary and Phytosanitary Affairs	Food and feed safety, veterinary and phytosanitary control, animal welfare;
Forest Administration	Forest management and protection;
Water Administration	Watercourse and waterways management and protection;

Public Administration Authorities of Montenegro	
Public authority	**Competence**
Directorate of Public Works	Preparatory, research and expert works regarding technical infrastructure and public bodies facilities, technical control in construction sector;
Environmental Protection Agency	Environmental monitoring, permitting, data collection and reporting;
Institute of Hydrometeorology and Seismology	Meteorological, hydrological, ecological and agrometeorological, seismic, parameters collection and forecasting;
Hydrocarbons Administration	Concession management for hydrocarbons exploration and production;
Administration for Maritime Safety and Port Management	Regulation, management and international cooperation regarding navigation safety in waterways and maritime traffic, concession management and supervision over ports;
Transport Directorate	Management and development of public roads, road control, permitting and tender's management;
Railway Directorate	Management and development of railways, permit issuing;
Administration for Inspection Affairs	Inspection and supervision in the areas of economy, tourism, labour, metrology, precious metals, games of chance, public procurement, health, social and child protection, ecology, forestry, water management, geology, mining and hydrocarbons, utilities, housing, geodesy, education, sports, cultural heritage, archiving and communications;
Secretariat for Legislation	Monitoring and improving the legal system, law harmonisation, professional assistance to legislators, law drafting and publication;
Sources: English names-https://www.gov.me/en/organizational-units, Competences - Uredba o organizaciji i načinu rada državne uprave, ("Službeni list Crne Gore", br. 049/22 od 06.05.2022)	

2.2 Technical standards implemented in the public administration information systems

Standards implemented with respect to IT service management:

1. ISO/IEC 20000-1:2011 (ISO 20000-1) *Information technology - Service management - Part 1. Service management system requirements:* **MEST ISO/IEC 20000-1:2019; ISO/IEC 20000-1:2018;**
2. ISO/IEC 20000-2:2012 (ISO 20000-2) *Information technology - Service management - Part 2. Guidance on the application of service management systems:* **MEST ISO/IEC 20000-2:2020;**
3. ISO/IEC 20000-3:2012 (ISO 20000-3) *Information technology - Service management - Part 3. Guidance on Scope definition and applicability of ISO/IEC 20000-1:* **MEST ISO/IEC 20000-3:2020;**

Standards implemented with respect to information security:

1. ISO/IEC 27000:2016 (ISO 27000) *Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary:* **MEST ISO/IEC 27000:2020; ISO/IEC 27000:2018;**
2. ISO/IEC 27011:2016 (ISO 27011) *Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations; (ISO 27001) Information technology - Security techniques - Information security management systems - Requirements:* **MEST ISO/IEC 27011:2009; ISO/IEC 27011:2016;**
3. ISO/IEC 27002:2013 (ISO 27002) *Information Technology - Security Techniques - Code of Practice for Information Security Controls:* **MEST EN ISO/IEC 27002:2020 (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015);**
4. ISO/IEC 27003:2010 (ISO 27003) *Information Technology - Security Techniques - Information Security Management Systems Implementation Guidance:* **ISO/IEC 27003:2017;**
5. ISO/IEC 27004:2016 (ISO 27004) *Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation:* **ISO/IEC 27004:2016;**
6. ISO/IEC 27005:2011 (ISO 27005) *Information technology - Security techniques - Information security risk management:* **MEST ISO/IEC 27005:2020;**
7. ISO/IEC 27006:2015 (ISO 27006) *Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems:* **MEST ISO/IEC 27006:2015;**
8. ISO/IEC 27007:2011 (ISO 27007) *Information technology - Security techniques - Guidelines for information security management systems auditing:* **ISO/IEC 27007:2020;**
9. ISO/IEC TR 27008:2011 (ISO 27008) *Information technology - Security techniques - Guidelines for auditors on information security controls:* **ISO/IEC TS 27008:2019;**
10. ISO/IEC 27010:2015 (ISO 27010) *Information technology - Security techniques - Information security management for inter-sector and inter-organisational communications:* **ISO/IEC 27010:2015;**
11. ISO/IEC 27011:2016 (ISO 27011) *Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations:* **MEST ISO/IEC 27011:2009; ISO/IEC 27011:2016/ Cor 1:2018;**
12. ISO/IEC 27013:2015 (ISO 27013) *Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1:* **ISO/ IEC 27013:2021;**

13. ISO/IEC 27014:2013 (ISO 27014) *Information technology - Security techniques - Governance of information security:* **ISO/IEC 27014:2020;**
14. ISO/IEC TR 27016:2014 (ISO 27016) *Information technology - Security techniques - Information security management - Organisational economics:* **ISO/IEC TR 27016:2014;**
15. ISO/IEC 27017:2015 (ISO 27017) *Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services:* **ISO/IEC 27017:2015;**
16. ISO/IEC 27018:2014 (ISO27018) *Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors:* **ISO/IEC 27018:2019;**
17. ISO/IEC TR 27019:2013 (ISO 27019) *Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry:* **MEST EN ISO/IEC 27019:2020; ISO/IEC 27019:2017;**
18. ISO/IEC 27023:2015 (ISO 27023) *Information technology - Security techniques - Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002:* **ISO/IEC TR 27023:2015;**
19. ISO/IEC 27032:2012 (ISO 27032) *Information technology - Security techniques - Guidelines for cybersecurity:* **ISO/IEC 27032:2012;**
20. ISO/IEC 27035-1:2016 (ISO 27035-1) *Information technology - Security techniques - Information security incident management - Part 1. Principles of incident management:* **ISO/IEC 27035-1:2016;**
21. ISO/IEC 27036-1:2014 (ISO 27036-1) *Information technology - Security techniques - Information security for supplier relationships - Part 1. Overview and concepts:* **ISO/IEC 27036-1:2021;**
22. ISO/IEC 27036-2:2014 (ISO 27036-2) *Information technology - Security techniques - Information security for supplier relationships - Part 2. Requirements:* **ISO/IEC 27036-2:2014;**
23. ISO/IEC 27036-3:2013 (ISO 27036-3) *Information technology - Security techniques - Information security for supplier relationships - Part 3. Guidelines for information and communication technology supply chain security:* **ISO/IEC 27036-3:2013;**
24. ISO/IEC 27038:2014 (ISO 27038) *Information technology - Security techniques - Specification for digital redaction:* **MEST EN ISO/IEC 27038:2017; ISO/IEC 27038:2014;**
25. ISO/IEC 27039:2015 (ISO 27039) *Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems (IDPS):* **ISO/IEC 27039:2015;**
26. ISO/IEC 27040:2015 (ISO 27040) *Information technology - Security techniques - Storage security:* **MEST EN ISO/IEC 27040:2017; ISO/IEC 27040:2015;**

27. ISO/IEC 27041:2015 (ISO 27041) *Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative methods:* **ISO/IEC 27041:2015;**
28. ISO/IEC 27042:2015 (ISO 27042) *Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence:* **MEST EN ISO/IEC 27042:2017; ISO/IEC 27042:2015;**
29. ISO/IEC 27043:2015 (ISO 27043) *Information technology - Information technology - Security techniques - Incident investigation principles and processes:* **MEST EN ISO/IEC 27043:2017; ISO/IEC 27043:2015;**
30. ISO 27799:2008 (ISO 27799) *Health informatics - Information security management in health using ISO/IEC 27002:* **MEST EN ISO 27799:2017; ISO 27799:2016;**

Standards implemented with respect to network security:

1. ISO/IEC 27033-1:2015 (ISO 27033-1) *Information technology - Security techniques - Network security - Part 1:* **Overview and concepts: ISO/IEC 27033-1:2015;**
2. ISO/IEC 27033-2:2012 (ISO 27033-2 *Information technology - Security techniques - Network security - Part 2. Guidelines for the design and implementation of network security:* **ISO/IEC 27033-2:2012;**
3. ISO/IEC 27033-3:2010 (ISO27033-3) *Information security - Security techniques - Network security - Part 3. Reference networking scenarios - Threats, design techniques and control issues:* **ISO/IEC 27033-3:2010;**
4. ISO/IEC 27033-4:2014 (ISO27033-4) *Information technology - Security techniques - Network security - Part 4. Securing communications between networks using security gateways:* **ISO/IEC 27033-4:2014;**
5. ISO/IEC 27033-5:2013 (ISO 27033-5) *Information technology - Security techniques - Network security - Part 5. Securing communications across networks using Virtual Private Networks (VPNs); ISO/IEC 27033-5:***2013;**
6. ISO/IEC 27034-1:2011 (ISO 27034-1) *Information technology - Security techniques - Application security - Part 1. Overview and concepts:* **ISO/IEC 27034-1:2011;**
7. ISO/IEC 27034-2:2015 (ISO 27034-2) *Information technology - Security techniques - Application security - Part 2. Organisation normative framework for application security:* **ISO/IEC 27034-2:2015;**

Standards implemented with respect to risk management:

1. ISO/IEC 31010:2009 (ISO 31010) *Risk management - Risk assessment techniques:* **MEST EN IEC 31010:2020; IEC 31010:2019;**
2. ISO 31000:2009 (ISO 31000) *Risk management - Principles and guidelines:* **MEST ISO 31000:2018;**

Standards implemented with respect to business continuity and disaster recovery standards:

1. ISO/IEC 27031:2011 (ISO 27031) *Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity:* **ISO/IEC 27031:2011;**
2. ISO/IEC 22301:2012 (ISO 22301) *Societal security - Business continuity management systems - Requirements:* **MEST EN ISO 22301:2020; ISO 22301:2019;**
3. ISO 22300:2012 (ISO 22300) *Societal security - Terminology:* **MEST EN ISO 22300:2019; ISO 22300:2021;**
4. ISO 22313:2012 (ISO 22313) *Societal security - Business continuity management systems - Guidance:* **MEST EN ISO 22313:2020; ISO 22300:2021;**

Standards implemented with respect to quality management:

1. ISO 9000:2015 (ISO 9000) *Quality management systems - Fundamentals and vocabulary:* **MEST EN ISO 9000:2016; ISO 9000:2015;**
2. ISO 9001:2015 (ISO 9000) *Quality management systems - Requirements:* **MEST EN ISO 9001:2016; ISO 9001:2015;**

Standards implemented with respect to software:

1. ISO/IEC 19770-1:2012 (ISO 19770-1) *Information technology - Software asset management - Part 1. Processes and tiered assessment of conformance:* **ISO/IEC 19770-1:2017;**
2. ISO/IEC 19770-2:2015 (ISO 197701-2) *Information technology - Software asset management - Part 2. Software identification tag:* **ISO/IEC 19770-2:2015;**

Standards implemented with respect to corporate governance:

1. ISO/IEC 38500:2015 (ISO 38500) *Information technology - Governance of IT for the organisation:* **ISO/IEC 38500:2015;**

Standards implemented with respect to certification and assessment:

1. ISO/IEC 15408-1/2/3:2005 - (ENISA) *Information technology - Security techniques - Evaluation criteria for IT security - Part 1. Introduction and general model (15408-1); Part 2. Security functional requirements (15408-2); Part 3. Security assurance requirements (15408-3):* **MEST EN ISO/IEC 15408-1:2020; ISO/IEC 15408-1:2009; MEST EN ISO/IEC 15408-2:2020; ISO/IEC 15408-1:2009; MEST EN ISO/IEC 15408-3:2020; ISO/IEC 15408-3:2008;**

2. ISO/IEC 29169:2016 *Information technology - Process assessment - Application of conformity assessment methodology to the assessment to process quality characteristics and organisational maturity:* **ISO/IEC 29169:2016;**
3. ISO/IEC TR 33018:2019 *Information technology - Process assessment - Guidance for assessor competency:* **ISO/IEC TR 33018:2019;**

Identified standards implemented with respect to trust services

a) ETSI EN 319 403 *Requirements for conformity assessment bodies assessing Trust Service Providers;*

b) ETSI EN 319 401 *General Policy Requirements for Trust Service Providers;*

c) x19 411: *Policy and security requirements for Trust Service Providers issuing certificates*

- EN 319 411-1: *General requirements*;
- EN 319 411-2: *Requirements for trust service providers issuing EU qualified certificates*;
- TR 119 411-4: *Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2*;

d) ETSI EN 319 421 *Policy and Security Requirements for Trust Service Providers issuing Electronic Timestamps*;

e) ETSI EN 319 102-1 *Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation*;

f) ETSI SR 019 510 *Scoping study and framework for standardisation of long-term data preservation services, including preservation of/with digital signatures*;

g) TS 119 441: *Policy requirements for TSP providing signature validation services*;

h) TS 119 431-1: *Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD/SCDev (remote signing)*;

i) TS 119 431-2: *Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation (remote signing)*;

j) EN 319 412 & TS 119 412 *Certificate Profiles (EN 319 412 and TS 119 412 are the same deliverables, but sometimes published as EN, sometimes published as TS to quickly include new features or corrections before a new EN is progressed)*;

- Part 1: *Overview and common data structures*;
- Part 2: *Certificate profile for certificates issued to natural persons*;
- Part 3: *Certificate profile for certificates issued to legal persons*;
- Part 4: *Certificate profile for web site certificates issued to organisations*;
- Part 5: *QCStatements*;

k) EN 319 422: *Time-stamping protocol and electronic time-stamp profiles*;

l) TS 119 432: *Protocols for remote digital signature creation*;

m) ETSI TS 119 511 *Policy & security requirements for trust service providers providing long-term preservation of digital signatures or unsigned data using signature techniques;*

n) ETSI TS 119 512 *Protocols for trust service providers providing long-term preservation of digital signatures or unsigned data using signature techniques*;

o) TR 119 100: *Guidance on the use of standards for signatures creation and validation*;

p) TS 119 101: *Policy and security requirements for applications for signature creation and signature validation*;

q) ETSI EN 319 521 *Policy and Security Requirements for Electronic Registered Delivery Service Providers*;

r) EN 319 522 *Electronic Registered Delivery Services*:

- Part 1: *Framework and Architecture*;
- Part 2: *Semantic Contents*;
- Part 3: *Formats*;
- Part 4: *Bindings*
  - 319 522-4-1: *message delivery binding*;
  - 319 522-4-2: *evidence and identification binding*;
  - 319 522-4-3: *capability/requirements binding*.

2.3 Technical standards planned to be implemented in the public administration information systems

Standards to be implemented

1. ISO/IEC 20000-4:2010 (ISO 20000-4) *Information technology - Service management - Part 4. Process reference model*
2. CEN TR 419 210: *"Applicability of CEN Standards to Qualified Electronic Seal Creation Device under the EU Regulation N°910/2014 (eIDAS)"*
3. CEN EN 419 221-5: *"Protection profiles for TSP Cryptographic modules - Part 5. Cryptographic Module for Trust Services"*
4. CEN EN 419 231: *"Protection profile for trustworthy systems supporting time stamping";*
5. CEN EN 419 241-1: *"Trustworthy Systems Supporting Server Signing - Part 1. General System Security Requirements"*
6. CEN EN 419 241-2: *"Trustworthy Systems Supporting Server Signing - Part 2. Protection profile for QSCD for Server Signing"*

7. ETSI TR 119 000: *"Electronic Signatures and Infrastructures (ESI); The framework for standardisation of signatures - overview"*
8. ETSI TS 119 403-3: *"Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3. Additional requirements for conformity assessment bodies assessing EU qualified trust service providers"*
9. ETSI TS 119 442: *"Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services"*
10. ETSI TS 119 495: *"Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366"*
11. ETSI TS 119 511: *"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques"*
12. ETSI TS 119 512: *"Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services"*
13. ETSI EN 319 521 (v1.1.1): *"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers"*
14. ETSI EN 319 522 series: *Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services;*
    - Part 1 (v1.1.1): *"Framework and Architecture"*
    - Part 2: *"Semantic contents"*
    - Part 3: *"Formats"*
    - Part 4: *"Bindings*:
      - Sub-part 1: "Message delivery bindings"
      - Sub-part 2: "Evidence and identification bindings"
      - Sub-part 3: "Capability/requirements bindings"
15. ETSI TS 119 524 (all parts): *"Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services"*
16. ETSI EN 319 531 (v1.1.1): *"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers"*
17. ETSI EN 319 532 series: *Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services;*
    - Part 1 (v1.1.1): *"Framework and Architecture"*
    - Part 2: *"Semantic contents"*
    - Part 3: *"Formats"*
    - Part 4: *"Interoperability profiles"*

18. ETSI TS 119 534 (all parts): *"Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Registered Electronic Mail Services" EN 301 549:* **"Accessibility requirements for ICT products and services"**
19. ETSI TS 119 612: *"Electronic Signatures and Infrastructures (ESI); Trusted Lists"*
20. ETSI TS 119 615: *"Electronic Signatures and Infrastructures (ESI); Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists"*
21. ETSI TR 103 684: *"Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services"*
22. ETSI TS 119 431-1 (v1.1.1): *"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1. TSP service components operating a remote QSCD/SCDev"*

V Recommendations on the prioritisation and implementation of standards and specifications on technical interoperability

1. Best practices on the implementation of standards at EU level

In order to achieve an effective and efficient mechanism for assessment, adoption and implementation of standards or specifications, five factors are of paramount importance: relevance, transparency, collaboration, compliance and monitoring, and training. These should be applied throughout the process of adoption of standards or specifications. They were identified in the ambit of the development of the Common Assessment Method for Standards and Specifications (CAMSS), presented below.[26]

Starting with **relevance**, this factor relates to the context in which the assessment process for new standards or technical specifications takes place. Adopting standards or specifications, which do not solve the issues faced by public authorities guarantees wasteful use of resources and that the standards will likely not be implemented or used. In order to be effective, a collection of standards needs to be adopted in light of the specific context and domain in which they will be put into use. The goal of the assessment should not be to select a "good" standard, but to choose one which answers the needs of the user, whomever he/she might be. In this sense, for a system for standards adoption to be relevant, it should be based on the needs expressed by the relevant stakeholders.

The next factor, **transparency** relates to the publicity of the assessment method. Having increased transparency in the process of selection and adoption of standards translates into increased mutual trust. This increased trust foments a collaborative environment for all stakeholders participating or affected by the standards to be adopted. The level of transparency is directly related to the communication and openness of all stages of the procedure. An important factor for enhanced transparency is the provision of justifications for the choices made, both in relation to methodology and to the adoption of a specific standard. Examples of actions which increase transparency include the addition of public consultations and the online publication of standards. A notable example of transparency is the United Kingdom's Standardisation Hub, discussed below.

To ensure an increased implementation of the adopted standards and specifications, it is fundamental that the adoption process occurs in a collaborative manner, thus the third factor is **collaboration**. All relevant stakeholders should be involved in the assessment of the

26 See: https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss

standard(s). They ought to be given the chance to express their needs and provide input in the assessment process. This involvement should be formalised and properly structured and it should start from the beginning of the assessment process. The involvement could take the form of a public consultation procedure or a public submission form.

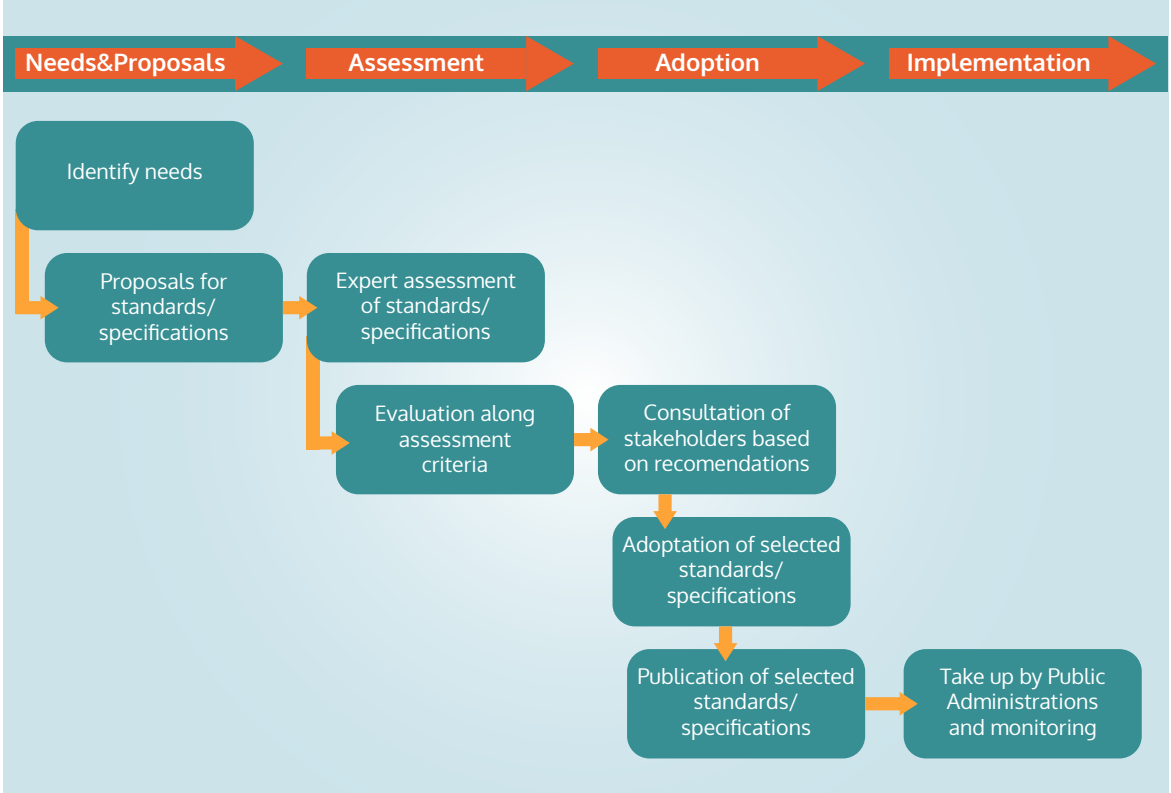
The penultimate factor is **compliance & monitoring**. This factor focuses on the control and tracking of the uptake of standards by public administrations, thereby allowing the evaluation of effectiveness of the method. The compliance and monitoring mechanisms should be set in the process of enforcement of standards or specifications. Additionally, the scope and extent which will delimit the monitoring should be defined in advance, as well. Different methods can be used to monitor adoption; examples of monitoring mechanisms include assessments of public administrations' architectures (Malta); online reports by researchers (Netherlands, Spain); online surveys (Netherlands) or remote audits (Slovakia). Obviously, if the output from the compliance and monitoring mechanisms is not followed by corrective action in the assessment, then this will lead to a significant decrease of efficiency.

The last factor in ensuring effectiveness and efficiency of the method for adoption of standards is **training**. The goal of training is to guarantee a common understanding, interpretation and consequently compliance with the adopted standards or specifications. If the adoption of standards involves interpretation of legislative acts, the importance of this training increases. The training can be either ex-ante or ex-post in relation to the adoption process, but it must seek to create a common knowledge and understanding of the standards.

Common Assessment Method for Standards and Specifications (CAMSS)

The CAMSS method represents a European Guide for assessing and selecting standards and specifications for eGovernment projects. The method seeks to represent an efficient assessment method that is need-based, transparent, collaborative and with mechanisms that ensure implementation. The goal of the method is to achieve interoperability and avoid vendor lock-in through a neutral and unbiased assessment of technical specification and standards in ICT. Thus, it attempts to ensure a high and consistent standard in the assessment of technical ICT standards and interoperability profiles. Additionally, it enables the reuse of the assessments made and serves for the continuous improvement of efficiency and effectiveness of the assessment. The method represents a move towards the Europeanisation of the assessments of standards, as it is compliant with Regulation 1025/2012 on European Standardisation.[27]

27 About Common Assessment Method for Standards and Specifications (CAMSS), Available at: https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/about



Source: Common Assessment Method for Standards and Specifications (CAMSS): Study on Adoption for Standards

The theoretical model is separated in four phases. These four phases are comprised of a total of eight consequential steps. The starting point for the assessment is the **"Needs & Proposal"** phase. It includes two steps: **"Identify needs"** and **"Proposals for standards/specifications."** In this sense, the adoption of standards or specifications should begin with the identification of the needs that public administration(s) has/have. Depending on what the specific needs are, different stakeholders (public administrators, standard providers, ministries, etc.) can propose standards and specifications that address those needs. Thus, in the first stage, the focus is on need-identification and gathering the proposals that fit those needs.

The second phase is **"Assessment"** and it covers the steps of **"Expert assessment of standards/specifications"** and **"Evaluation along assessment criteria."** Having identified the relevant standards and specifications, the model moves towards their assessment. The aim of the assessment is to appraise the selected standards *vis-à-vis* an established set of criteria. The model suggests the application of the principle from Recommendation 22 of the European Interoperability Framework: "Use a structured, transparent, objective and common approach to assessing and selecting standards and specifications." Take into account relevant EU recommendations and seek to make the approach consistent across borders."[28] The first step sets out to establish an expert group, which will have the task to evaluate the proposed standards and specifications. In its evaluation, the expert group will examine the standards against the established set of criteria. The output of the expert group can comprise a set of recommendations.

28 Available at: https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf

Moving to the **"Adoption"** phase, it involves three steps. Firstly, **"Consultation of stakeholders based on recommendations,"** secondly, **"Adoption of selected standards/specification"** and lastly, **"Publication of selected standards/specifications"**. After the assessment and before the adoption, the model provides for possibility of launching public consultation. The purpose of this consultation is to gain feedback from stakeholders on the recommendations. After the feedback is integrated, the adoption can be formalised by the relevant body. The last step involves publication of the adopted standards or specifications as a list that is either recommended or mandatory. After the publication, the adoption by public bodies can begin.

The last phase is **"Implementation,"** and it has only one step, which is **"Take-up by Public Administrations and monitoring."** After the publication, it is expected that the recommended or mandatory standards or specifications are adopted in practice by public authorities in the implementation of their ICT solutions, irrespective of whether they are bought or build in-house. In the adoption process, it is possible to include a monitoring procedure. This can be done with the aim to determine whether there is an uptake in the implementation of standards by the public administration bodies. This monitoring can be organised in different ways, as it can vary in its implementation and as to what is monitored. The main question for monitoring is whether the standard is mandatory or enforceable, or only recommended.[29]

UK's Open Standards (ex-Standards Hub)

The UK Open Standards is the overhauled Standards Hub, and it represents an open and transparent adoption method for standards for public administrations. It was refreshed in 2015 to increase the simplicity and encourage citizen participation.[30] The method has five consequential steps, and it results in the adoption of an open standard. The choice for open standards is based on the advantages they bring: no or low costs; open and collaborative design process; no licensing restrictions and lastly, compatibility with other open source and proprietary solutions (no vendor lock-in problem).

The steps in choosing a standard are:

1. Anyone can suggest a problem and a possible open standard solution;
2. The Open Standards team decides on a 'challenge owner' to lead the assessment on a suggested open standard solution;
3. The challenge owner assesses the open standards regarding its suitability;
4. The challenge owner writes a proposal for the Open Standards Board;
5. The Open Standards Board approves the open standards, as either mandatory or recommended, for use for the government.

29 See: https://joinup.ec.europa.eu/sites/default/files/document/2018-05/CAMSS%20Study%20on%20adoption%20methods%20for%20standards%20%28Final%20report%29.pdf

30 Blog: Government Technology at: https://governmenttechnology.blog.gov.uk/2015/03/06/standards-hub-simpler-and-clearer/

The first step is for anyone to suggest a problem found in government and a solution which an open standard can solve. This suggestion is called a 'challenge'. The challenge ought to include: a problem; who are the users and what are their needs; the benefits of solving the problem with an open standard (justification); and lastly, a suggestion of one or more open standards as a solution. The suggestions are made through a GitHub repository.[31]

After the suggestion phase, the Open Standards team, representing a panel of technology experts, decides on whether the challenge suggested is to be taken to the community for open discussion. In this open discussion anyone can view any challenge, comment or suggest an alternative standard. In this space, open discussions in the form of suggestions, alternative standards or feedback are encouraged. Subsequently, the Open Standards team assigns a 'challenge owner'. The challenge owner is a volunteer who leads the work to transform a challenge to a proposal.

After their selection, the challenge owner is guided through the role's requirements and through the open standards process. He/she must carry out an assessment of the suggested open standard as to its suitability. This assessment should also include the extents to which the standard follows the Open Standards principles.[32] The Open Standards Board has 47 questions to use in the assessment. These questions are based on the CAMSS method described above. They cover seven topics regarding the standard: its specifications; its implementation in organisations; its openness and availability; its versatility and flexibility; the effect and benefits for the end user; how organisations can maintain the standard's use; and lastly, how is the standard related to other European standards.

In the penultimate step, the challenge owner must write a formal proposal to the Open Standards Board.[33] The community can review and comment on the drafts of the proposal. The proposal should include information about the standard, how it will meet the user's needs, a summary of the answers to the abovementioned 47 questions, the predicted benefits and opportunities of using the standard and how the standards can help interoperability. The proposal is sent to the Open Standards Board for approval.

Lastly, the Board will decide on the adoption of the standard. The standard can be either accepted, accepted with conditions or rejected. While acceptance is clear, acceptance with conditions means that the proposal will be sent back to the challenge owner with questions and suggestions for amendments. The proposal can be also rejected. To decide on the adoption, the Board will evaluate based on whether it meets the user needs, if it gives equal opportunity to open source and proprietary software, is mature enough and usable by all government organisations and widely used by suppliers, if it supports the use of open data and aligns with the open data principles and the digital strategies of the government. Additionally, information from workshops and community comments will also be taken into account.[34]

31 Open Standards GitHub repository: https://github.com/co-cddo/open-standards
32 Open Standards principles: https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles#open-standard---definition
33 Open Standards Board: https://www.gov.uk/government/groups/open-standards-board
34 Guidance-Choosing open standards for government: https://www.gov.uk/guidance/choosing-open-standards-for-government#challenge-owner

1.1 Mapping and analysis of strategic documents and standards adopted by standardisation organisations, ICT industry and consortia

Within the current study, a variety of documents and standards with respect to the adoption of standards and enhancing the overall level of technical interoperability in Montenegro has been analysed. Besides the abovementioned documents, a brief overview of the analysed documents and standards will be made in this section, as follows:

- Recommendation on technical implementation of eIDAS Regulation[35] - this strategic document elaborated by the European Union Agency for Cybersecurity (ENISA) presents guidance on how the eIDAS assessment regime can be strengthened based on the current regime of the eIDAS regulation, analysing the available legal framework and instruments to support actions towards a harmonised conformity assessment scheme for QTSP/QTS. Besides, the report both analyses the gaps with respect to such a harmonised scheme and proposes concrete actions towards a harmonised eIDAS QTSP/QTS conformity assessment scheme. In the report, for example, it is stated that IAF MLA driven accreditation scheme based on [ISO/IEC 17065] (potentially supplemented by [ETSI EN 319 403]) is a candidate for non-EU economies to base their domestic QTSP/QTS certification scheme on, particularly for other QTS than issuing qualified certificates. Besides, such economies may expand and finalise the ETSI EN 319 403-based scheme by the establishment of a harmonised, specific and complete certification scheme, as the latter will lay down a sufficient level of technical details, as well as the exact set of controls and control objectives that the CAB will have to use to conduct a conformity assessment of a QTSP/QTS against more generic legal provisions. This may be facilitated by the fact that domestic legislations may reference standards as binding normative documents (contrary to the eIDAS Regulation). Overall, the scheme based on ISO/IEC 17065 and supplemented by ETSI EN 319 403 is said to be applicable to any type of TSP/TS for being assessed to any type of standard, technical specification or regulation - it is completely independent of the eIDAS Regulation. The EA recommended eIDAS scheme is adding to this generic scheme under the eIDAS Regulation as the normative documents against which the QTSP/QTS need to be assessed in terms of conformity. In this regard, any non-EU economy, including Montenegro, may act similarly by adding its own regulatory or technical specifications as normative criteria against which domestic TSP/TS need to be assessed in terms of conformity.[36]
- Trusted e-ID infrastructures and services in EU[37] - this report by ENISA provides a list of general recommendations to e-Government service providers and Member State Regulators, as well as specific recommendations for Trust Service Providers. Although

35 Available at: https://www.enisa.europa.eu/publications/towards-a-harmonised-conformity-assessment-scheme-for-qtsp-qts

36 European Union Agency for Cybersecurity (ENISA), Recommendations for technical implementation of the eIDAS Regulation, 2019, page 17.

37 Available at: https://www.enisa.europa.eu/publications/trusted-eid

the report dated from 2013, it provides valuable recommendations regarding the provision of e-Government services. For instance, one of the recommendations to Member State Regulators envisages that "trust services should be developed with European scope, complying with European Regulation, which should be promoted. This practice would solve all interoperability and security issues in a common and trusted way. e-Government service providers should accept and prioritise TSPs audited by a recognised independent body confirming that TSPs fulfil the obligations laid down in the Regulation."[38]

- eIDAS compliant eID Solutions (Security Consideration and the Role of ENISA)[39] - the current report by ENISA provides an overview of the legislative framework under eIDAS for electronic identification, presents the landscape of notified and pre-notified eID schemes and identifies key trends in the electronic identification field. Moreover, it discusses preliminary security considerations and recommendations related to the underlying technologies used for eID means and makes a proposal on the role that ENISA could play in the eIDAS compliant eID ecosystem.

1.2 Mapping and analysis of specifications

- Overview of Standards (Specifying formats of advanced electronic signatures and seals)40 - this report by ENISA focuses on the assessment of sustainability of the updated set of European Norms (ENs) on advanced signature formats, aiming to describe the differences with the previous Technical Specification (TSs).
- Technical specifications v.1.241 - these specifications are the latest set of eIDAS -compliant technical specifications, endorsed by Opinion №5/2019 of the Cooperation Network on 27th of September 2019 and consisting of four documents, each addressing concrete issues, namely: eIDAS Message Format v.1.2; eIDAS Interoperability Architecture v.1.2.; eIDAS Cryptographic Requirement v.1.2; eIDAS SAML Attribute Profile v.1.2.

38 European Union Agency for Cybersecurity (ENISA), Trusted e-ID Infrastructures and services in EU, 2013, page 9.
39 Available at: https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions
40 Available at: https://www.enisa.europa.eu/publications/assessment-of-standards-related-to-eidas-i
41 Available at: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eIDAS+eID+Profile

VI Process of selection and adoption of standards and specifications

1. Analysis of the procedures for selection and adoption of standards in Montenegro

The procedures for standard selection and adoption in Montenegro are regulated by three legislative acts: the Law on Standardisation (hereinafter: LS),[42] Decree on Establishing the Institute for Standardisation of Montenegro (hereinafter: Decree),[43] and the Statute of the Institute for Standardisation of Montenegro (hereinafter: ISME Statute), where both documents (Decree and Statute) will be harmonised with the new LS.[44] In Montenegro, the responsible authority for standardisation is the Institute for Standardisation of Montenegro (hereinafter: ISME), as it is responsible for the adoption of domestic standards and related documents, and for "ensuring the compliance between these national standards and documents with the European and international standards."[45] The application of standards is not mandatory, although in cases where a technical regulation refers to such standard, the latter is mandatory and is to be implemented as a technical regulation by the respective bodies.[46]

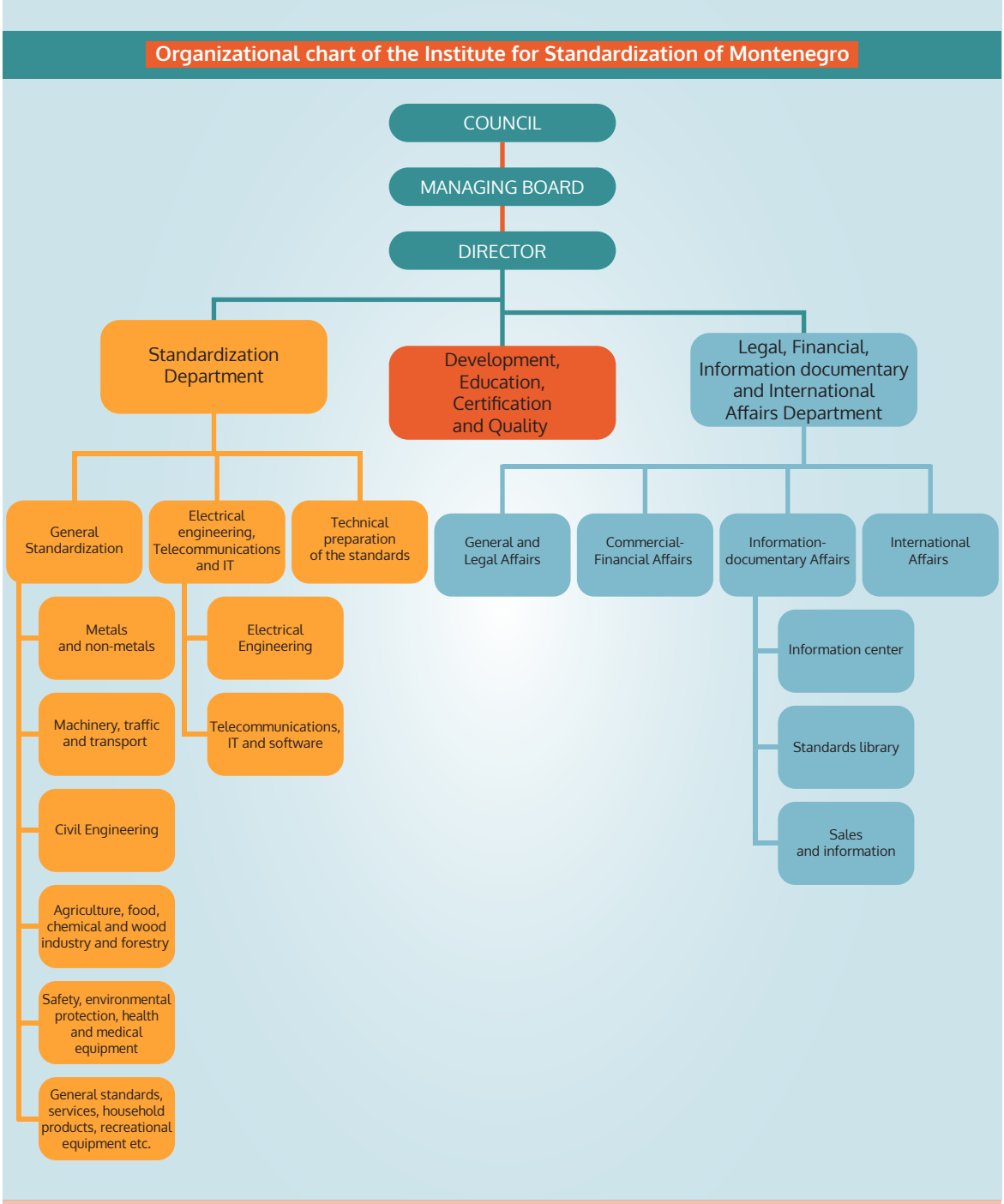
The provisions contained in the abovementioned legislative acts can be separated in four areas pertaining to the standard adoption process: principles and objectives regarding standardisation; organisation and powers of the Institute for Standardisation of Montenegro (ISME); the procedure for adoption, application and publication of standards and relation with other certification bodies; and other supplemental norms. In the following paragraphs, each of the three main areas for standardisation will be grouped and presented, followed by a textual and policy analysis.

Starting with the principles and objectives of standardisation, they are enshrined in arts. 3 and 4 of the Law of Standardisation and art. 16 of the ISME Statute. Beginning with art. 3 LS, it sets out the principles on which standardisation will be based in Montenegro. Those are: voluntary participation (para. 1), consensus (para. 2), common interest (para. 3), transparency (para. 4), coherence (para. 5), consideration of European and international standards (para. 6 and 9), most-favoured nation and national treatment principles (para. 7), avoidance of technical barriers to international trade (para. 8) and lastly, preference for standards of

42 Zakon o standardizaciji, "Službeni list CG", br. 13/08 od 26.02.2008
43 Odluka o osnivanju Instituta za standardizaciju Crne Gore, "Službeni list CG", br. 21/07 od 13.04.2007
44 Statut Instituta za standardizaciju Crne Gore, "Službeni list CG" 29/2008 od 06.05.2008.
45 Law on Standartisation, Article 1, available at: https://isme.me/en/zakon-o-standardizaciji_p5047.html, last accessed on 06.12.2021
46 Law on Standartisation, Article 16, available at: https://isme.me/en/zakon-o-standardizaciji_p5047.html, last accessed on 06.12.2021

performance (para. 10). The objectives of standardisation are laid down in art. 4 of LS and are: protection of life, health and environment (para. 1), promotion of quality (para. 2), promotion of uniform technical basis (para. 3), promotion of production and trade through international harmonisation (para. 4), and avoidance of technical barriers to international trade (para. 5). Lastly, art. 16 of ISME Statute prescribes that the performance of ISME shall be public, and it sets out the conditions under which publicity will be achieved.

Moving to the organisation of ISME, the Institute has three governing bodies: the Council, Managing Board and the Director (art. 7 of LS and of Decree). The Council directs and administers the work of the Institute. It is composed of 15 members, seven of which are appointed by the Government of Montenegro. The other eight are appointed by the members of ISME, taking into consideration that they ought to be representative of the composition of the Institute members (art. 8, para. 3 of the Decree). It is important to note, from the reading of the legislation, that this requirement seems to apply only to the councilmen/women appointed by the Institute's members and not to the ones appointed by the Government. Additionally, no quota system for the representation is to be found in either one of the three documents. This arrangement seems problematic for two reasons. Firstly, having a significant part of the councilmen/women appointed by the government might impact the independence and consensus-based approach necessary for the adoption of standards. Secondly, having no quota system in place for non-governmentally appointed members can additionally serve to skew the bias of the Council in its work. The members of the Council are appointed for a four-year term with the possibility of one reappointment (art. 8 of the Decree).



Source: Organisational Chart of the Institute for Standardisation of Montenegro.[47]

47 available at: https://isme.me/en/download/file/page-section/195, last accessed 21.12.2021

As to its tasks, the Council appoints its own chairman, approves the Statute of ISME (subject to governmental approval), appoints two members to the Managing Board and approves the entirety of the Board, approves the annual work programme and regulations regulating ISME (subject to consent by the Government), approves the yearly contracts between ISME and the Government, approves the annual performance report and financial statements, and lastly, selects an independent auditor (art. 9 of the Decree). Furthermore, the Council adopts its own rules of procedure, appoints and dismisses its chairman, adopts the Statute at the proposal of the Board (subject to consent by the Government), performs other duties as enshrined in either the Law, Decree or Statute and lastly, it can establish temporary bodies for selected tasks (art. 25 of the Statute). The chairman convenes and chairs the meetings and performs other duties under the Statute and Rules of Procedure. He/she is selected by majority voting for four years and can be reappointed once (art. 10 of the Decree). The Council has two voting procedures, where each member has one vote. Usually, it votes by simple majority with at least 2/3 of the members present. If the vote is on the Statute of ISME, a qualified majority of 2/3 is needed for approval. Despite this, art. 28 of ISME Statute provides that the rules of procedure also describe the decision-making process and the performances of the Council.[48] Lastly, the same articles describes that the Chairman of the Board and the Director take part in the Council meetings but have no voting rights.

Moving to the Managing Board, it is composed of four members and a chairman. They are appointed for four years with the possibility of one reappointment, and they should be distinguished experts, scientists or economists. Two of them are nominated by the Government, two by the Council and one by the staff of the Institute. The chairman of the Board is chosen among the members by simple majority (art. 11 and 12 of the Decree and art. 30 of the Statute). The Board is responsible for making decisions on the ISME's operations, proposes the annual work programme, plan and contract with Government, considers the performance reports and financial statements, arranges meetings of the Council, approves the ISME rules for standardisation and national mark of conformity, approves the internal organisation of the Institute (proposed by Director), approves the annual membership fee, price list of standards and documents and services, and performs other duties under the Law, Decree or Statute (art. 13 of the Decree). Additionally, it adopts its own rules of procedure,[49] proposes the Statute to the Council, appoints and dismisses the Director and takes decisions on international cooperation (art. 33 of the Statute).

The last governing body is the Director. As stated above he/she is appointed by the Board for four years through an open competition, with the possibility of one reappointment (art. 14 of the Decree and art. 38 of the Statute). The requirements for the position are to be a Montenegrin citizen, at least 18-years-old, have a master's degree and at least five years of managerial experience or nine years of work experience at performing with the university level of education and, lastly, not have a criminal record (art. 39 of the Statute). The duties of the Director include organising and managing the work of ISME, representation, ensuring the legality of the functions of the Institute, approving regulations on adoption or annulment

48 Poslovnik o radu Skupštine, 22/I/20, 11.12.2020
49 Poslovnik o radu Upravnog odbora, 26/V/2020, 28.10.2020

of Montenegrin standards, suggesting regulations on internal organisation to the Board, management of assets of the Institute, enforcement of decisions of the Council and the Board, management of contractual relations between staff and the institute, establishment of ad hoc bodies for specifics tasks, preparation of financial statements and other duties under the three governing acts (art. 15 of the Decree). Additionally, the Director appoints representatives to international bodies (art. 40 of the Statute).

At the time of writing, the Institute is separated in two departments and one independent division under the Director. The first department is the Standardisation Department, which is separated in three divisions: General Standardisation, Electrical Engineering and Technical Preparation of Standards. The first two are further separated in sub-divisions depending on the economic sector in which standardisation is needed. The second department is the Legal, Financial, Information - Documentary and International Affairs Department. It has four divisions, one for each of its responsibilities. The independent division is Development, Education, Certification and Quality.[50]

As to the activities and powers of the institute, they are regulated in art. 6 of LS, art. 4 of the Decree and arts. 9-13 of ISME Statute. The Institute adopts Montenegrin standards, ensures compliance with international standards, maintains a register of standards in all phases, can participate in international preparation of standards, cooperates internationally in the area of standardisation, performs international standardisation obligations, disseminates domestic standards to the public, prepares technical regulations and annual plans for domestic standard adoption, and acts as an information centre (art. 6 of LS). Furthermore, it builds capacity for standardisation, promotes the enforcement of standards, establishes cooperation with other bodies (public or private) in the field of standardisation, cooperates with other domestic standardisation bodies, adopts domestic standards, European and international ones, acts as a point of contact for WTO/TBT and Codex Alimentarius, approves the Montenegrin conformity mark use and implements the contracts between ISME and Montenegrin Government (art. 4 of the Decree). Lastly, it engages professional organisations and associations for the creation of domestic standards (art. 10 of ISME Statute). The institute is independent and non-profit organisation for standardisation established by the Law on Standardisation ("Official Gazette of Montenegro", No. 13/08) by Decision on the Establishment of the Institute ("Official Gazette of the Republic of Montenegro", No. 21/07) and by the Statute of the Institute for Standardization of Montenegro ("Official Gazette of Montenegro", No. 29/08, 057/19).

Having described the organisation and activities of ISME, it is possible to move to the procedure for adoption of standards. Starting with international standards, Montenegro is a member of the WTO since 2012,[51] therefore the Agreement on Technical Barriers to Trade is binding on it. Consequently, Annex 3: Code of Good Practice for the Preparation, Adoption and Application of Standards provides that where international standards exist, they should be used as basis for domestic standards, with the exceptions when they would be ineffective or inappropriate.[52]

50 Organisational Chart of ISME, available at https://isme.me/en/download/file/page-section/195, last accessed 20.12.2021

51 WTO Members and Observers, available at: https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm, last accessed 21.12.2021

52 Agreement on Technical Barriers to Trade, available at: https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm#annexIII, last accessed 21.12.2021

Thus, when ISME decides to create a standard in a given sector, if an international standard exists or is about to be adopted, the ISME should use it, unless it would be ineffective or inappropriate. The same is enshrined in art. 9, paras. 13-15 of ISME Statute. As to European standards, ISME is an affiliate of CEN-CENELEC. Thus, as an affiliate member, it is obliged to withdraw any domestic standards conflicting with European ones and to adopt the latter in which it has participated as domestic ones.[53]

As to the adoption of domestic standards, the procedure is codified in Chapter IV of the Law on Standardisation. The domestic procedure starts with a notification in the ISME's official journal that a procedure for adoption of a standard has begun (art. 10, para. 2 of LS). Per art. 12 of LS, before the adoption takes place, ISME must allow minimum 60 days for comments on the draft (para. 1), although that period can be waived in case of urgent problems (para. 3). Any interested party can obtain a copy of the draft upon request, although fees can be charged for service (para. 2). In its procedure, ISME has to take into account the comments received and has to reply to them and provide justifications for any deviation from international standards. Montenegrin standards are differentiated with the MEST acronym and are adopted and published in Montenegrin (art. 13 and 14 of the Law on Standardisation).

Looking at the legislative acts together, three main problems, which warrant further examination, are identified in the process of adoption and modification of standards in Montenegro. These are related to legal clarity, lack of certainty and independence.

Starting with legal clarity, reading together the Law on Standardisation, Decree establishing ISME and Statute of ISME, it becomes apparent that there are some issues. One significant problem that obfuscates the reading and understanding of the regime for adoption of standards in Montenegro is that articles pertaining to the same matters are spread among the three documents. Sometimes the articles are copy-pasted between the acts, on other occasions there are two articles with the same subject-matter, yet with different content. Examples of that are art. 6 of LS, art. 4 of Decree, art. 9 of Statute; art. 7 of LS, art. 7 of Decree, art. 23 of Statute; art. 8 of LS, art. 5 of Decree, art. 21 of Statute; art. 16 of Decree, arts. 17-18 of Statute; arts. 8-10 of Decree, art. 24-29 of Statute; arts. 11-13 of Decree, arts. 30-37 and arts. 14-15 of Decree, art. 38-40 of Statute. The present structure creates a situation of lack of legal clarity, which goes against the principles of transparency and openness inherent in standardisation. In this light, it is worth pointing out that legislative streamlining has been implemented. However, this streamlining should have legal clarity and avoidance of duplication in mind, whereby the provisions contained in the documents are organised and structured in an open and easy and to understand way. Thus, increasing the openness of the process, as enshrined in art. 3, para. 4 of LS.

Moving to the second issue, it concerns the steps presented in the process of adoption of Montenegrin standards. While the situation pertaining to international and European standards is rather clear, as explained above, there is again a lack of clarity with the procedure for adoption of domestic standards. Despite having three documents, only in the shortest one

53 About CEN: Affiliates, available at: https://standards.cencenelec.eu/dyn/www/f?p=CEN:9, last accessed 21.12.2021 and CEN-CENELEC GUIDE 12: The concept of Affiliation with CEN and CENELEC Edition 4, 2016-06-15, p. 7

-the Law of Standardisation (only 23 articles) - is the procedure for the adoption of standards described. As identified above, the procedure is described in Chapter IV of the Law and according to it, the procedure starts with an "official journal notification of the initiation of a procedure for adoption of a Montenegrin standard, and, if necessary, for related documents". The problem with this approach to starting the procedure is that there is no mention of a needs-based assessment for the creation of standards. As described in Chapter V of the present study, adopting standards based on an identified need is fundamental, both for the usefulness of the standard and for its adoption in practice. Otherwise, adopting a standard not needed creates the possibility that the standard is not used, at best, and, at worst, it can create market barriers and distort market functioning, both domestically and internationally. Therefore, further clarification is needed in this sense, focusing on a needs-based approach. This is especially so considering that a needs-based approach is not to be found in the principles which guide Montenegrin standardisation (art. 3 LS).

A further issue is to be found with the topic of public participation and openness of the process. While transparency and voluntary participation of interested parties are part of the guiding principles (art. 3, paras. 1 and 4 of LS) of the Law on Standardisation, it seems that there are several possible barriers to openness to be found in Chapter IV. Firstly, in art. 12 of LS, despite the obligation of the Institute to provide a copy of the draft standard upon request, this is effectively put behind a paywall, which can limit the transparency of the process depending on the size of the fees being charged. A further problem is that the latter seems to be set by the Managing Board and approved by the Government. Moreover, notwithstanding the obligation in art 12, para. 1 of LS to leave a minimum 60-day period for submission of comments from interested parties, this period can be "shortened or eliminated in the case urgent problems related to safety, health or environment arise by virtue of art. 12, para. 3 of LS. The problem to be found here is that nowhere in the texts is it defined what "urgent" means. This leaves open door for the procedure for comments to be waived rather easily. Additionally, it is not mentioned who is the responsible authority within the ISME for taking this decision. Lastly, in providing replies to comments received in line with art. 12, para. 4 of LS, it seems that the Institute has an obligation to provide justifications only when it deviates from international standards and not for other choices made in the standard to be adopted. The last two provisions that raise concerns as to the openness of the procedure are arts. 15 and 16 of the Statute. Art. 15 of the Statute states that it is up to the discretion of the Director to define what documents and data are considered as business secret. While art. 16 of the Statute creates a rather confusing and onerous procedure where the Chairman of the Council and of the Managing Board and the Director have to approve public information activities in written form. While these rules do not create a problem per se, their ambiguity leaves a rather big discretion to ISME in taking decisions regarding public knowledge and participation, thereby not working to the idea of openness and transparency. Consequently, it would be advisable to improve the procedure for standards adoption by limiting ISME's discretion through stricter qualitative criteria.

The last general issue concerns the question of government participation. While according to art. 1 of the Decree, the ISME is an independent non-profit organisation under domestic law, the government has a significant control over its operations. Firstly, it is important to note that

the government is referred to as the "founder" in most of the cases where it is referenced (art. 5, para 2 of LS, art. 2 of the Statute). This, while not affecting the substantive content of the norms, it affects the easiness of reading the documents. Moving to the substantive provisions, the Government of Montenegro appoints seven out of 15 members of the Council (art. 8 of the Decree); consents the Statute; consents to the annual work programmes and plans for standards, and regulations for development of ISME (art. 9 of the Decree); nominates two out of five members of the Board (art. 11 of the Decree, art. 30 of the Statute); consents to the price lists for standards and other documents and publications (art. 13, para. 9 of the Decree) and consents to the yearly Contracts of Performance between ISME and itself (art. 9, para. 5 of the Decree). While the last point is not contentious, considering that the Contract of Performance functions to regulate the financing of the Institute, the rest gives the Government a significant amount of decision-making and approval, both as to the organisation and to the financing of the Institute. The abovementioned provisions go directly against the idea of independence in the operation of the Institute and can conflict with the idea of open collaboration and consensus in standard making, since the needs of the government and the needs of standard users might not conflate. The following major issues have been identified:

- Problem 1: Among the three existing legislative acts articles are copy-pasted, some are modified, while others are not. All of them are relatively difficult to read and lack clarity. Thus, it is clear that legislative base needs streamlining and unification;
- Problem 2: No clear procedure for adoption of domestic standardisation has been identified, which is problematic and might create issues when mass standardisation begins;
- Problem 3: Too much governmental influence over work of the Institute is noticed.

A possible solution for the problems mentioned above is streamlining of the existing legal framework, establishing a methodology for standardisation, and setting up the grounds for creating an independent institute. These three steps will ensure clear domestic procedures, solid legal basis and independent oversight when it comes to Montenegro's technical interoperability.

1.1 Analysis of primary and secondary legislation

The primary and secondary legislation with respect to the technical interoperability and e-Governance includes a majority of legal acts, governing different aspects, namely - trust services and electronic identification, Single Information System for Data Exchange (SISEDE), process of adoption of domestic standards, etc.

The new National Interoperability Framework (NIF) of Montenegro adopted in 2019 and based on the new European Interoperability Framework of 2017 provides a set of standards, recommendations and guidelines regarding the communication and exchange of information between them. The purpose of the NIF is to support the public administration authorities in enhancing their level of interoperability in order to guarantee provision of electronic

administrative services. Section 3.1.1 of the NIF named "Determining and selecting standards and specifications" refers to the general steps which need to be followed for selection and adoption of standards and specifications. It has to be noted that the NIF is based on the European Interoperability Framework (EIF), as the purpose of the latter is "to provide guidance to public administrations on the design and update of national interoperability frameworks (NIFs), or national policies, strategies and guidelines promoting interoperability", as well as to "contribute to the establishment of the digital single market by fostering cross-border and cross-sectoral interoperability for the delivery of European public services".

One of the most important legal acts with regard to enhancing the level of technical interoperability in Montenegro is the Law on Electronic Government, adopted in 2020. In accordance with the Law on Electronic Government, all public authorities shall provide electronic services to citizens and organisation through the use of Single Information System for Electronic Data Exchange (SISEDE). However, in order to provide these services, the authorities are obliged to comply with certain domestic, European and international technical standards and specifications prescribed by the Ministry of Public Administration , which is the supervising authority with respect to the application of the Law on Electronic Government. In this respect, Art. 9 of the Law enshrines that all bodies which provide electronic administration services through SISEDE should meet certain technical and other requirements in order to be able to use the system, and that these requirements are prescribed by the Ministry. The regime and general requirements for integration with and use of SISEDE by the government bodies are enshrined in the Law on Electronic Government, including the components and management of SISEDE, access to it, taxes for provision of electronic administrative services, penalties for violation of provisions of the law (for example, for not meeting the requirements under Art. 9), etc. In addition, more exhaustive requirements for managing, functioning and use of SISEDE are prescribed by the Regulation on the management method and other issues of relevance for the functioning of the Single System for Electronic Data Exchange, adopted on the basis of Art. 22, para. 4 of the Law on Electronic Government.

With respect to trust services and electronic identification, the law governing these matters in Montenegro is the Law on Electronic Identification and Electronic Signature, adopted in 2017 and amended in 2019. According to Art. 1 of the Law, the latter regulates the regime of all trust services (electronic signatures, including advanced and qualified electronic signatures, electronic registered delivery services, electronic seals and website authentication) in legal transactions and in all proceedings, as well as the electronic identification scheme and requirements for recognition of other economies' electronic identification means. Some of the most notable amendments in the Law made in 2019 concern separation of electronic identification and trust services, elimination of the word "certification" and better description of the process of standardisation of electronic identification.[54] With regard to the Law on Electronic Identification and Electronic Signature, a number of bylaws have been adopted to regulate different aspects of services provided, including, but not limited to:

54 Digital Public Administration factsheet 2020 - Montenegro, 2020, Available at: https://joinup.ec.europa.eu/sites/default/files/inline-files/Digital_Public_Administration_Factsheets_Montenegro_vFINAL.pdf

- Rulebook on the manner of assessing compliance of qualified devices for creating electronic signatures and electronic seals and on the content of list of certified qualified devices for creating electronic signatures and electronic seals. Adopted in 2020 in relation to Article 19 of the Law on Electronic Identification and Electronic Signature, the Rulebook regulates the manner for assessing the compliance of qualified devices for creating electronic signatures and electronic seals and the content of list of certified qualified devices for creating electronic signatures and electronic seals. Regarding the abovementioned compliance, Art. 2 of the Rulebook prescribes that the compliance of these devices with the requirements set in Article 19 of the Law on Electronic Identification and Electronic Signature shall be assessed based on the standards set forth in Annex 1 of the Rulebook. The standards enshrined are the following ones:

  - ISO/IEC 15408 - *Information technology - Security techniques - Evaluation criteria for information technology security, Parts 1 to 3 as follows bellow*:
    - ISO/IEC 15408-1:2009 - *Information technology - Security techniques - Evaluation criteria for information technology security, - Part 1 ISO 2009*,
    - ISO/IEC 15408-2:2008 - *Information technology - Security techniques - Evaluation criteria for information technology security, - Part 2 ISO 2008*,
    - ISO/IEC 15408-3:2008 - *Information technology - Security techniques - Evaluation criteria for information technology security, - Part 3 ISO 2008*;
  - ISO/IEC 18045:2008 - *Information technology - Security techniques - Methodology for IT security evaluation*;
  - ETSI EN 419 211 - *Protection Profiles for Secure Signature Creation Devices, Parts 1 to 6 - namely*:
    - EN 419211-1:2014 - *Protection Profiles for Secure Signature Creation Devices - Part 1: Overview*,
    - EN 419211-21:2014 - *Protection Profiles for Secure Signature Creation Devices - Part 2 Device with key generation*,
    - EN 419211-31:2014 - *Protection Profiles for Secure Signature Creation Devices - Part 3 Device with key import*,
    - EN 419211-41:2014 - *Protection Profiles for Secure Signature Creation Devices - Part 4 Extension for device with key generation and trusted communication with certificate generation application*,
    - EN 419211-51:2014 - *Protection Profiles for Secure Signature Creation Devices - Part 5 Extension for device with key generation and trusted communication with signature creation application*, and

- EN 419211-61:2014 - *Protection Profiles for Secure Signature Creation Devices - Part 6 Extension for device with key import and trusted communication with certificate signature creation application.*

- Rulebook on the manner of providing electronic trust services and qualified electronic trust services for public administration authorities. This Rulebook has been adopted pursuant to Art. 5, para. 3 of the Law on Electronic Identification and Electronic Signature and regulates the manner in which the Ministry of Public Administration provides electronic and qualified electronic trust services, including the rules that need to be adopted for provision of such service (Art. 4-5), as well as the order for issuing and revoking certificates of civil servants in the public administration (Art. 6-12). In accordance with Art. 2 of the Rulebook, when providing such electronic and qualified electronic trust services, the Ministry shall act in accordance with ETSI EN 319 401 standard and other standards referred to by that standard, as well as the Law on Electronic Identification and Electronic Signature.

- Rulebook on more detailed requirements that qualified electronic trust service provider must meet - the Rulebook is adopted pursuant to Art. 34, para. 2 of the Law on Electronic Identification and Electronic Signature prescribing the requirements for provision of qualified trust services by qualified trust service providers. The provisions of the Rulebook envisage specific standards which qualified trust service providers (QTSPs) must meet to provide the services, namely:

  - ETSI EN 319 401
  - EN 319 421
  - ETSI EN 319 411-1
  - ETSI EN 319 411-2

  The provided standards are related to different obligation of the QTSPs foreseen both in the Law on Electronic Identification and Electronic Signature and in the Rulebook. These obligations include elaboration of practical rules (Art. 2), elaboration of plan for termination of service provision (Art. 4, last paragraph), elaboration of personal data protection plan (Art. 5, para. 2), the expertise of its employees (Art. 7, para. last) and the measure for prevention of forgery (Art. 9).

  - ETSI TS 119 312

  These technical specifications enshrined in the Rulebook concern the systems that the QTSP uses. In particular, all QTSPs are obliged to comply with them to guarantee that 1) they use trustworthy systems and products which are protected against unauthorised modification and ensure technical and cryptographic security of the processes (Art. 8), and 2) the qualified certificates storage systems used by the QTSPs meet technical specifications.

- Rulebook on measures and activities for protection of certificate for electronic signature and electronic seal - this Rulebook prescribes organisational and technical

measures which should be applied by trust service providers and public authorities for protection of certificates for electronic signatures and electronic seals, and the data related to the signatory and the creator of the electronic seals. According to Art. 3 of the Rulebook, the following measures, standards and technical specification must be applied:

- general measures and activities contained in ETSI EN 319 401, *Electronic Signatures and Infrastructures (ESI); General Requirements for Trust Service Providers.*
- measures to protect schemes for services of issuance of certificates for electronic signature, electronic seal and website authentication, contained in the following standards:
  - ETSI EN 319 411-1, *Electronic Signatures and Infrastructures (ESI); Policy and safety/security requirements for Service Providers issuing certificates: General requirements,*
  - ETSI EN 319 411-2, E*lectronic Signatures and Infrastructures (ESI); Policy and safety/security requirements for Service Providers issuing certificates: Requirements for Service Providers issuing qualified EU certificates,*
  - ETSI EN 319 412-1, *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and Common Data Structures,*
  - ETSI EN 319 412-2, *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons,*
  - ETSI EN 319 412-3, *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons,*
  - ETSI EN 319 412-4, *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for Website Certificates,*
  - ETSI EN 319 412-5, *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: Qualified Certificate Statement.*
- measures to protect schemes for electronic time stamp issuance services contained in the following standards:
  - ETSI EN 319 122-1, *Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures*
  - ETSI EN 319 122-2, *Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures*
  - ETSI TS 119 122-3, *Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 3: Incorporation of Evidence Record Syntax in CAdES*
  - ETSI EN 319 132-1, *Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures*

- ETSI EN 319 132-2, Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; - Part 2: Extended XAdES signatures
- ETSI EN 319 142-1, Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building Blocks and PAdES baseline signatures
- ETSI EN 319 142-2, Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles
- ETSI TS 119 142-3, Electronic Signatures and Infrastructures (ESI); ETSI TS 119 142-3 PAdES digital signatures; Part 3: PAdES Document Time-stamp digital signatures (PAdES-DTS)
- ETSI EN 319 162-1, Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers
- ETSI EN 319 162-2, Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers
- ETSI EN 319 102-1, Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ETSI TS 119 172-1, Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents

- Cryptographic data protection measures, in accordance with the following standards:
  - ETSI TR 119 300, Electronic Signatures and Infrastructures (ESI); Guidance on the use of standards for cryptographic suites
  - ETSI TS 119 312, Electronic Signatures and Infrastructures (ESI); Cryptographic suites

- Rulebook on detailed requirements that must be met by a qualified electronic registered delivery service - this Rulebook prescribes specific obligations, but not any concrete standards that should be followed by electronic trust service providers and public authorities when providing a qualified electronic registered delivery service. However, there is one reference to such standards, as Art. 2 enshrines that the identity of the sender might be established, besides the other means provided, “in any other ways in accordance with the minimum technical standards and accompanying procedures referred in Art. 60 of the Law on Electronic Identification and Electronic Signature. On the other hand, the referred technical standards and accompanying procedures are related to the determination of the assurance levels of the electronic identification scheme.
- Rulebook on detailed content and manner of keeping records of electronic trust service providers and register of qualified electronic trust service providers - the Rulebook prescribes what kind of information should be contained in the records of the

electronic trust service providers (Art. 4) and the registers of the qualified electronic trust service providers (Art. 6). The only standard in this Rulebook is applicable to both service providers, as Art. 4 and Art. 6 enshrine that these records/registers should contain data related to the **certificate type designation in accordance with** ETSI EN 319 412-5 **and** ETSI EN 319 411-2 **(6.6.1).**

Regarding the electronic identification (eID), two bylaws governing the latter have been identified, namely:

- Rulebook on technical and operational requirements related to node - point of connecting electronic identification schemes and process of establishing electronic identification schemes interoperability framework. Although Art. 1 of the Rulebook enshrines that the later regulates the technical and operational requirements related to the node, no concrete standards have been provided. Instead, Art. 3 states that European and international standards should be applied with regard to technical and operational requirements related to the node. Besides, Art. 6 enshrines that "the process of establishing the interoperability framework is implemented by applying the following European practice and international standards:

  - eIDAS Message Format;
  - eIDAS Interoperability Architecture;
  - eIDAS Cryptographic Requirements for interoperability on eIDAS;
  - eIDAS Security Assertion Markup Language Attribute Profile;

  The mentioned Technical Specifications v.1.2 are the latest set of eIDAS-compliant technical specifications, endorsed by Opinion No.5/2019 of the Cooperation Network on 27th of September 2019.

- Rulebook on minimum technical standards and accompanying procedures relating to which assurance levels for electronic identification schemes are determined

1.2 Available reports and other documents

The available reports and other documents which has served the analysis are listed below:

- Public Administration Strategy of Montenegro 2022-2026
- Strategy for Information Society Development 2020
- Digital Public Administration Factsheet Montenegro 2020
- eGovernment Benchmark Report 2021
- eIDAS Compliant eID Solutions (Security consideration and the role of ENISA)

1.3 Analysis of the procedures for selection of specifications

The process for selection of specifications is prescribed in the NIF of Montenegro, as well as in its primary and subsidiary legislation in force. Institute for Standardisation of Montenegro (ISME) is responsible for the adoption of domestic standards and related documents. In order to "ensure the compliance between these national standards and documents with the European and international standards"[55] it is supposed that ISME is working in close relationship with international standardisation organisations. For instance, the following ones: International Standardisation Organisation (ISO), International Electrotechnical Commission (IEC), International Telecommunications Union (ITU). Moreover, ISME already collaborates with the EU standardisation organisations mentioned below.

The European Telecommunications Standards Institute (ETSI) is responsible for developing standards for telecommunications, broadcasting and other electronic communications networks and services. The European Committee for Standardisation (CEN) provides a platform for development of European Standards and other technical documents in relation to various kinds of products, materials, services and processes. The European Committee for Electrotechnical Standardisation (CENELEC) prepares voluntary standards in the electrotechnical field. The Directorate-General for Informatics (DG DIGIT) of the European Commission through the Interoperable Europe initiative reinforces interoperability policy in the public sector. The European Interoperability Framework (EIF)[56] gives specific guidance on how to set up interoperable digital public services. The adoption of principals and the conceptual model set in EIF is a prerequisite to ensure interoperability of public services in Montenegro with the public services in other EU member states. DirectorateGeneral for Communications Networks, Content and Technology (DG CONNECT) of the EC develops and implements policies to make Europe to fit the digital age. Last, but not least, the European Union Agency for Cybersecurity (ENISA) is the Union's agency dedicated to achieving a high level of common cybersecurity across Europe. ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies. ENISA publications provide essential guidance regarding the applicable standards related to eID, trust services, and cybersecurity in general.[57]

With regards to the recommendations set out in the EIF and the NIF of Montenegro regarding technical interoperability, as already stated, they both endorse the use of open specifications, where available, to ensure technical interoperability when establishing European public services.[58] In order for this to be achieved, Montenegro should select and adopt certain technical specifications that will guarantee the interoperability of all public systems and

55 Law on Standardisation, Article 1, available at: https://isme.me/sr_ME/download/file/page-section/102, last accessed: 29.04.2022.
56 More available at: https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail, last accessed: 29/04/2022.
57 More information available at: https://www.enisa.europa.eu/publications#c3=2012&c3=2022&c3=false&c5=publicationDate&reversed=on&b_start=0, last accessed: 29.04.2022.
58 Recommendation 33 of the European Interoperability Framework

services with the European systems. To achieve such interoperability, you can use CAMSS and its solutions, at it is the European guide for assessing and selecting standards and specifications for an eGovernment project.[59] Overall, there is no unified procedure for selection of technical specifications which should be followed by the government, however there are guidelines elaborated by different standardisation and other organisations which might be helpful.[60]

1.4 Identification of concrete norms related to the selection and adoption of standards and specifications for technical interoperability

The process of selection and adoption of technical standards and specification for enhancing the level of technical interoperability of Montenegro is described in both the legislation of Montenegro and in specific guidelines and other reports by European and international organisations such as ETSI. The main EU legal act governing the European standardisation activities, including the identification and use of technical standards and specifications, is Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council.[61] Besides promoting the participation of SMEs and domestic public authorities within the process of standard development, the Regulation also provides requirements for identification of ICT technical specifications in Annex II of the latter. As stated in Art. 13 of the Regulation, the provided requirements must be met in case the Commission decides to identify ICT technical specifications that are not domestic, European or international standards. However, ISME should strive to transpose European standards and technical specifications in order to enhance the interoperability of their services and systems, and to make a step towards the implementation of cross-border/boundary provision of European public services.

Montenegro government needs to follow the policies and principles set by European Commission and its respective bodies, DG DIGIT and DG CONNECT, EIF in particular, related to interoperability. A development and adoption of Montenegro National Interoperability Framework aligned with EIF will streamline interoperability of Montenegro administrative information systems with those of the EU member states. The mandatory standards could be listed in an Interoperability Rulebook and later on updated with the changes and adoption of new standards by the relevant EU standardisation bodies. A Cybersecurity Rulebook could present the set of security standards related to administrative information systems. A list of recommended standards to be adopted is presented in Appendix II. ISME needs to decide on the timeframe of such implementation.

59 https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss
60 Understanding ICT Standardisation: Principles and Practice, ETSI, 2018, Available here: https://www.etsi.org/images/files/Education/ETSI_STF-515_slides_consolidated_04032019.pdf
61 Available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025, last accessed 03/05/2022

With regard to the abovementioned rulebooks the Ministry of Public Administration needs to develop Interoperability and Cybersecurity Rulebooks or similar to state the abovementioned standards and specifications as mandatory.

1.5 Summary of the findings

Montenegro government created a framework of legal acts, rulebooks and standards to provide interoperability. The Institute for Standardisation of Montenegro (ISME) is responsible for development of standards. The procedure of selection and adoption of standards by ISME is not clear. It is recommended to improve it.

International and European standards are voluntary. So are the standards adopted by Montenegro. To ensure interoperability at EU level Montenegro government should follow the recommendations of the EC policy making authorities (DG DIGIT and DG CONNECT). To ensure technical interoperability Montenegro competent institutions needs to apply requirements and recommendations of ENISA and adopt standards issued by EU standardisation bodies ETSI, CEN, and CENELEC. In particular, more attention should be put on adoption of CEN standards listed in Appendix II. In requirements listed in documents related to development of administrative information systems and their interoperability, standards must be enumerated explicitly as mandatory. Standards related to design, development, support and maintenance and exploitation of administrative information systems need to be listed as mandatory in appropriate rulebooks.

VII Minimum technical standards and specifications for enabling data exchange and document security in cross-border/boundary provision of public services

1. Overview of the process of mapping minimum technical standards and specifications

Interoperable Europe[62] is the initiative of the European Commission for a reinforced interoperability policy in the public sector. It is committed to introducing a new cooperative interoperability policy for Europe that will transform the public administrations and help them in their digital transformation. The initiative is supported by the Digital Europe programme. It continues and expands the mission of the now completed ISA² programme. To ensure data exchange and document security in cross-border/boundary provision of public services government of Montenegro needs to follow the requirements and recommendations of EC for a reinforced interoperability policy in the EU. Interoperable Europe represents the policy framework for pursuing, supporting, developing and promoting interoperability across the European Union.

The whole data policy environment, e.g. Open Data Directive, Data Act, and Data Governance Act, is becoming one of the crucial sectors the EU has been focusing on. Semantic interoperability is seen as a key area to support data spaces, which do not only need pure data-exchange technologies and standards, but also have to be adapted constantly. Supporting open source for the public sector is of paramount importance.

The EIF[63] gives guidance, through a set of recommendations, to public administrations on how to improve governance of their interoperability activities, establish cross-organisational relationships, streamline processes supporting end-to-end digital services, and ensure that existing and new legislation do not compromise interoperability efforts.

62 The European Commission launched Interoperable Europe, the new policy framework for interoperability in the EU, available at: https://openforumeurope.org/interoperable-europe/, last accessed 04/04/2022

63 European Interoperability Framework, available at: https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf, last accessed: 04/04/2022

1.1 Minimum technical standards and specifications for enabling data exchange

Following ISO 20614:2017 Information and documentation - Data exchange protocol for interoperability and preservation (DEPIP) enables data exchange. The Data Exchange Protocol for Interoperability and Preservation aims at facilitating interoperability between a digital archive and information systems of its partners: producers who have created the documents themselves (Originating Agency), intermediaries who are acting on behalf of producers and are not responsible for the intellectual content per se (Transferring Agency), consumers (Consumer) and control authorities (Control Authority). This document provides a framework for data exchange between systems. It is based on the OAIS Reference model. It is generic and may be adapted to all types of information, whether printed or in a born-digital format.

According to Regulation EU 910/2014 Article 3 (35) "'electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording, i.e. administrations in a state and across EU exchange documents, not data. Exchanged data are part of the exchanged documents.

1.2 Minimum technical standards and specifications for document security

There are two main standard clusters related to document security - ISO/IEC 29500 and ISO 32000. These standards are much more important for software developers working on creation of word processing solutions rather than to public administration officers who are users of such kind of solutions.

ISO/IEC 29500 (all Parts) specifies a family of XML schemas, collectively called Office Open XML, which define the XML vocabularies for word-processing, spreadsheet, and presentation documents, as well as the packaging of documents that conform to these schemas.

The goal is to enable the implementation of the Office Open XML formats by the widest set of tools and platforms, fostering interoperability across office productivity applications and line-of-business systems, as well as to support and strengthen document archival and preservation, all in a way that is fully compatible with the existing corpus of Microsoft® Office1 documents.

ISO 32000 is the family of ISO standards that defines the core PDF specification, as identified by the PDF version number. All other PDF subset specifications depend on a specific core PDF version.

The basic requirements for document security in intra-economy and cross-border/boundary provision of public services are regulated with EU Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

2. List of identified minimum technical standards

2.1 for enabling data exchange in cross-border/boundary provision of public services

According to Regulation EU 910/2014 Article 3 (35) "'electronic document' means any content stored in electronic form, in particular text or sound, visual or audiovisual recording, i.e. administrations in a state and across EU exchange documents, not data. Exchanged data are part of the exchanged documents.

Administrations publish open data according to the adopted policies and legislation of EU and particular jurisdictions. The most popular open data formats are: csv, odf, html xml, and json. Other open data formats are: xls, xlsx, doc, docx, rdf, txt, jpg, png, gif, tiff, pdf, ods, odt, tsv, geojson. Open Government Data Standard 2.0[64] was published in 2016 and recommends XML+CSD or JSON.

2.2 for enhancing document security in cross-border/boundary provision of public services

E-Document exchanges across borders/boundaries should be signed electronically. To ensure document security in cross-border/boundary provision of public services EC provides a notification tool.[65] The notification procedure is described at https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Notification+Tool?preview=/467109182/467109188/EU%20Trust%20Services%20Dashboard%20-%20Notifier%20user%20guide.pdf.

Montenegro authorities adopted a set of technical standards recommended by ENISA and presented in Appendix I. These are the minimum technical standards that allow internal use of e-signatures and electronic documents within Montenegro.

To make sure that cross-border/boundary provision of public services will be implemented successfully Montenegro administration needs to adopt the technical standards listed in Appendix II.

64 Open Government Data Standard 2.0, https://joinup.ec.europa.eu/collection/open-government/solution/open-government-data-standard-20

65 Notification tool, https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Notification+Tool

VIII General conclusions & recommendations

1. Summary and analysis of the findings

Technical interoperability is the foundation for implementation of Once-Only Principle (OOP). From December 2023, the Once-Only Principle will allow public administrations in Europe to reuse, or share, data and documents that people have already supplied in a transparent and secure way. Thus, base registers and other key data sources in every Member State will need to share information in real-time, across borders. EC adopted Single Digital Gateway Regulation (SDGR)[66] to simplify access to cross-border administrative procedures initiated online by citizens or companies based in another EU member state.

Government of Montenegro does not need to wait until accession to implement EC regulations and directives. The administrative bodies should operate as the economy is an EU member state. It is not enough to have a legal framework in place. It is much more important to apply it in practice. Regarding the technical interoperability Montenegro adopted a substantial set of standards listed in Appendix I. In addition, standards listed in Appendix II need to be adopted. It is essential that all these standards are implemented in all stages of future ICT projects related to digital transformation of the central government and municipality administrations of Montenegro.

2. General recommendations for boosting the level of technical interoperability readiness

Montenegro is working toward accession to the EU. Therefore, it is essential to follow EU's digital strategy[67] that aims to make digital transformation work for people and businesses, while helping to achieve its target of a climate-neutral Europe by 2050. Open source could be instrumental to achieving internal and cross-border/boundary technical interoperability. Under the theme 'Think Open', EC Open-Source Software Strategy 2020-2023[68] has set out a vision for encouraging and leveraging the transformative, innovative and collaborative power of open source, its principles and development practices.

The analysis of the process of selection and adoption of standards and specifications in section VI above shows that procedures to create standards if they do not originate from EC or ISO are rather ambiguous and unclear. Therefore, the Law on Standardisation needs improvements

66 Single Digital Gateway Regulation (SDGR), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0001.01.ENG&toc=OJ:L:2018:295:TOC

67 Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en, last accessed 04/04/2022

68 Available at: https://ec.europa.eu/info/departments/informatics/open-source-software-strategy_en, last accessed 04/04/2022

in this direction, particularly by providing clear procedure for adoption of new domestic standards.

2.1 Interoperability

In order for Montenegro to achieve full digital interoperability of all central government and municipality bodies and their information systems, all administration information systems (AIS) in Montenegro will need to connect with the Single Information System for Electronic Data Exchange (SISEDE). In this regard, it should be pointed out that within the performing of this analysis, no technical barriers regarding such connecting have been identified. The results of the conducted analysis did show that Montenegrin authorities have the technical capacity to achieve such integration of SISEDE, however, allocation of additional resources and political willingness will be needed. In addition, the integration of SISEDE with the Single Digital Gateway (SDG) shall be performed by the Ministry of Public Administration, resulting in interconnection between SDG and SISEDE, and establishing the latter as a single point of contact. The latest report by the Directorate General for Informatics (European Commission) lays out domestic initiatives (political and legal) related to digitalisation and interoperability of public administrations which have been put in place. Furthermore, the report presents worldwide developments rather than only EU ones, which will provide Montenegro with additional solutions.[69] In addition, specifications to ensure technical interoperability are also included.

Interoperable Europe[70] is the initiative of the European Commission for a reinforced interoperability policy. Enhanced interoperability will be necessary to unlock the potential of data usage and reuse for improved public services, to enable cross-border/boundary collaboration, and to support the sector-specific policy goals set by the Commission for the future. Interoperable Europe programme supports the development of solutions in the area of interoperability. A set of solutions[71] is already operational and can be reused free of charge. More solutions will be made available continuously.

2.2 Standards

With respect to technical standards which are adopted and those that need to be adopted by the Institute for Standardisation, both have been listed in two appendixes to this study - Appendix I (adopted standards) and Appendix II (to be adopted). Nevertheless, it should be highlighted that the sole adoption of the listed standards will not be enough for enhancing the level of technical interoperability of the administration in Montenegro. Additionally, these standards

69 Bachmaier, P., Bleys, E., Chiarelli, F. and others, 'State-of-play report on digital public administration and interoperability 2021', Luxembourg: Publications Office of the European Union, 2021, available at: https://joinup.ec.europa.eu/sites/default/files/news/2021-12/State-of-play%20report%202021_vFinal.pdf, last accessed: 20/04/2022

70 ISA² - Interoperability solutions for public administrations, businesses and citizens, https://ec.europa.eu/isa2/news/new-level-cooperation-isa□C2□B2-building-interoperable-europe_en#

71 ISA² - Interoperability solutions for public administrations, businesses and citizens, https://ec.europa.eu/isa2/solutions_en

related to management of design, development, implementation, training, maintenance and support of e-services must be applied by the respective central government and municipal administrative bodies. The comprehensive implementation of the listed technical standards in the information systems of the administrations should be closely monitored and controlled both by the managements of these administrations and the Ministry of Public Administration.

2.3 Trust Services

eID and e-signature solutions were implemented in Montenegro. A promotion campaign will be instrumental to increase awareness and stimulate their usage. On the other side, government of Montenegro and Ministry of Public Administration need to accelerate the introduction of e-services that bring added value to citizens and businesses. A good tool to promote e-services is to make them free of charge or to reduce the fees for e-services to the half of the regular (paper based) fee. It is essential to connect to European eIDAS network.

2.4 eIDAS Node

Concerning the possible adoption of cross-border/boundary electronic identification scheme, it is recommended that Montenegro should not wait for accession in the EU to implement the latter, as it could be implemented in the pre-accession period. In order to enable Identity Providers to connect to the eIDAS Network, Montenegro needs to appoint a Single Point of Contact. In compliance with the European legislation on electronic identification, the government of Montenegro must use the Connecting Europe Facility (CEF) Building block to deploy an eIDAS Node. The CEF eID Building block represents a set of services (including software, documentation, training and support) provided by the European Commission and endorsed by the Member States, which helps public administrations and private Service Providers to extend the use of their provisions of services to citizens from other European countries (including the WB economies). Such provision is possible through the use of mutual recognition of electronic identification (eID) schemes (including smartcards, mobile and log-in), allowing citizens of one EU member state to use their national eIDs for secure online access provided in other member states. The mutual recognition of eID schemes across Europe is mandated by the eIDAS Regulation, which enshrines that by 29 September 2018 all online public services requiring electronic identification assurance corresponding to a level of “substantial” or “high” must be able to accept the notified eID schemes of other EU member states. Therefore, public administrations are obliged to comply with these requirements. With regards to the technical specifications for eIDAS compliance, the latter are available at eIDAS eID Profile.[72]

72 Available at: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile, last accessed 04/04/2022

Appendix I - Adopted standards

No.	Standard	Implemented	Note
IT service management standards			
1	**ISO/IEC 20000-1:2011** (ISO 20000-1) Information technology - Service management - Part 1: Service management system requirements	**MEST ISO/IEC 20000-1:2019** 11.12.2019 **ISO/IEC 20000-1:2018** 14.09.2018	This document specifies requirements for an organisation to establish, implement, maintain and continually improve a service management system (SMS). The requirements specified in this document include planning, design, transition, delivery and improvement of services to meet the service requirements and deliver value. This document can be used by: a) a customer seeking services and requiring assurance regarding the quality of those services; b) a customer requiring a consistent approach to the service lifecycle by all its service providers, including those in a supply chain; c) an organisation to demonstrate its capability for planning, design, transition, delivery and improvement of services; d) an organisation to monitor, measure and review its SMS and the services; e) an organisation to improve planning, design, transition, delivery and improvement of services through effective implementation and operation of an SMS; f) an organisation or other party performing conformity assessments against the requirements specified in this document; g) a provider of training or advice in service management. The term "service" as used in this document refers to the service or services in the scope of the SMS. The term "organisation" as used in this document refers to the organisation in the scope of the SMS that manages and delivers services to customers. The organisation in the scope of the SMS can be part of a larger organisation, for example, a department of a large corporation. An organisation or part of an organisation that manages and delivers a service or services to internal or external customers can also be known as a service provider. Any use of the terms "service" or "organisation" with a different intent is distinguished clearly in this document.

No.	Standard	Implemented	Note
2	**ISO/IEC 20000-2:2012** (ISO 20000-2) Information technology - Service management - Part 2: Guidance on the application of service management systems	**MEST ISO/IEC 20000-2:2020** 18.12.2020	This document provides guidance on the application of a service management system (SMS) based on ISO/IEC 20000-1. It provides examples and recommendations to enable organisations to interpret and apply ISO/IEC 20000-1, including references to other parts of ISO/IEC 20000 and other relevant standards.
3	**ISO/IEC 20000-3:2012** (ISO 20000-3) Information technology - Service management - Part 3: Guidance on Scope definition and applicability of ISO/IEC 20000-1	**MEST ISO/IEC 20000-3:2020** 11.03.2020.	This document includes guidance on the scope definition and applicability to the requirements specified in ISO/IEC 20000-1. This document can assist in establishing whether ISO/IEC 20000-1 is applicable to an organisation's circumstances. It illustrates how the scope of an SMS can be defined, irrespective of whether the organisation has experience in defining the scope of other management systems. The guidance in this document can assist an organisation in planning and preparing for a conformity assessment against ISO/IEC 20000-1. Annex A contains examples of possible scope statements for an SMS. The examples given use a series of scenarios for organisations ranging from very simple to complex service supply chains. This document can be used by personnel responsible for planning the implementation of an SMS, as well as assessors and consultants. It supplements the guidance on the application of an SMS given in ISO/IEC 20000-2. Requirements for bodies providing audit and certification of an SMS can be found in ISO/IEC 20000-6 which recommends the use of this document.
4	**ISO/IEC 20000-4:2010** (ISO 20000-4) Information technology - Service management - Part 4: Process reference model	ISO/IEC 20000-4 is not in the list of Montenegro standards	

No.	Standard	Implemented	Note
Information security standards			
1	**ISO/IEC 27000:2016** (ISO 27000) Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary	**MEST ISO/IEC 27000:2020** 18.12.2020 **ISO/IEC 27000:2018** 07.02.2018	ISO/IEC 27000:2018 provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organisation (e.g. commercial enterprises, government agencies, not-for-profit organisations). The terms and definitions provided in this document - cover commonly used terms and definitions in the ISMS family of standards; - do not cover all terms and definitions applied within the ISMS family of standards; and - do not limit the ISMS family of standards in defining new terms for use.
2	**ISO/IEC 27011:2016** (ISO 27011) Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations (ISO 27001) Information technology - Security techniques - Information security management systems - Requirements	**MEST ISO/IEC 27011:2009** (14.12.2009) **ISO/IEC 27011:2016**	The scope of this Recommendation | International Standard is to define guidelines supporting the implementation of information security management in telecommunications organisations. The adoption of this Recommendation | International Standard will allow telecommunications organisations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security property.
3	**ISO/IEC 27002:2013** (ISO 27002) Information Technology - Security Techniques - Code of Practice for Information Security Controls	**MEST EN ISO/IEC 27002:2020 (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)** (18.12.2020)	Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)

No.	Standard	Implemented	Note
4	**ISO/IEC 27003:2010** (ISO 27003) Information Technology - Security Techniques - Information Security Management Systems Implementation Guidance	**ISO/IEC 27003:2017** (12.04.2017)	ISO/IEC 27003:2017 provides explanation and guidance on ISO/IEC 27001:2013.
5	**ISO/IEC 27004:2016** (ISO 27004) Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation	**ISO/IEC 27004:2016** (15.12.2016)	ISO/IEC 27004:2016 provides guidelines intended to assist organisations in evaluating information security performance and effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001:2013, 9.1. It establishes: a) monitoring and measurement of information security performance; b) monitoring and measurement of the effectiveness of an information security management system (ISMS) including its processes and controls; c) analysis and evaluation of the results of monitoring and measurement. ISO/IEC 27004:2016 is applicable to all types and sizes of organisations.
6	**ISO/IEC 27005:2011** (ISO 27005) Information technology - Security techniques - Information security risk management	**MEST ISO/IEC 27005:2020** (18.12.2020)	This document provides guidelines for information security risk management. This document supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this document. This document is applicable to all types of organisations (e.g. commercial enterprises, government agencies, non-profit organisations) which intend to manage risks that can compromise the organisation's information security.

No.	Standard	Implemented	Note
7	**ISO/IEC 27006:2015** (ISO 27006) Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems	**MEST ISO/IEC 27006:2015** 24.07.2015	ISO/IEC 27006:2011 specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification. The requirements contained in ISO/IEC 27006:2011 need to be demonstrated in terms of competence and reliability by any body providing ISMS certification, and the guidance contained in ISO/IEC 27006:2011 provides additional interpretation of these requirements for any body providing ISMS certification.
8	**ISO/IEC 27007:2011** (ISO 27007) Information technology - Security techniques - Guidelines for information security management systems auditing	**ISO/IEC 27007:2020** 21.01.2020.	This document provides guidance on managing an information security management system (ISMS) audit programme, on conducting audits, and on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011. This document is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.
9	**ISO/IEC TR 27008:2011** (ISO 27008) Information technology - Security techniques - Guidelines for auditors on information security controls	**ISO/IEC TS 27008:2019** 14.01.2019	This document provides guidance on reviewing and assessing the implementation and operation of information security controls, including technical assessment of information system controls, in compliance with an organisation's established information security requirements including technical compliance against assessment criteria based on the information security requirements established by the organisation. This document offers guidance on how to review and assess information security controls being managed through an Information Security Management System specified by ISO/IEC 27001. It is applicable to all types and sizes of organisations, including public and private companies, government entities, and not-for-profit organisations conducting information security reviews and technical compliance checks.

No.	Standard	Implemented	Note
10	**ISO/IEC 27010:2015** (ISO 27010) Information technology - Security techniques - Information security management for inter-sector and inter-organisational communications	**ISO/IEC 27010:2015** 10.11.2015	SO/IEC 27010:2015 provides guidelines in addition to the guidance given in the ISO/IEC 27000 family of standards for implementing information security management within information sharing communities. This International Standard provides controls and guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organisational and inter-sector communications. It provides guidelines and general principles on how the specified requirements can be met using established messaging and other technical methods. This International Standard is applicable to all forms of exchange and sharing of sensitive information, both public and private, domestically and internationally, within the same industry or market sector or between sectors. In particular, it may be applicable to information exchanges and sharing relating to the provision, maintenance and protection of an organisation's or economy's critical infrastructure. It is designed to support the creation of trust when exchanging and sharing sensitive information, thereby encouraging the international growth of information sharing communities.
11	**ISO/IEC 27011:2016** (ISO 27011) Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations	**MEST ISO/IEC 27011:2009** 14.12.2009 **ISO/IEC 27011:2016/Cor 1:2018** 29.08.2018	The scope of this Recommendation | ISO/IEC 27011:2016 is to define guidelines supporting the implementation of information security controls in telecommunications organisations. The adoption of this Recommendation | ISO/IEC 27011:2016 will allow telecommunications organisations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security property.
12	**ISO/IEC 27013:2015** (ISO 27013) Information technology - Security techniques - Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	**ISO/IEC 27013:2021** 25.11.2021	This document gives guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for organisations intending to: a) implement ISO/IEC27001 when ISO/IEC 20000-1 is already implemented, or vice versa; b) implement both ISO/IEC27001 and ISO/IEC 20000-1 together; or c) integrate existing management systems based on ISO/IEC27001 and ISO/IEC 20000-1. This document focuses exclusively on the integrated implementation of an information security management system (ISMS) as specified in ISO/IEC 27001 and a service management system (SMS) as specified in ISO/IEC 20000-1.

No.	Standard	Implemented	Note
13	ISO/IEC 27014:2013 (ISO 27014) Information technology - Security techniques - Governance of information security	**ISO/IEC 27014:2020** 15.12.2020	This document provides guidance on concepts, objectives and processes for the governance of information security, by which organisations can evaluate, direct, monitor and communicate the information security-related processes within the organisation. The intended audience for this document is: - governing body and top management; - those who are responsible for evaluating, directing and monitoring an information security management system (ISMS) based on ISO/IEC 27001; - those responsible for information security management that takes place outside the scope of an ISMS based on ISO/IEC 27001, but within the scope of governance. This document is applicable to all types and sizes of organisations. All references to an ISMS in this document apply to an ISMS based on ISO/IEC 27001. This document focuses on the three types of ISMS organisations given in Annex B. However, this document can also be used by other types of organisations.
14	ISO/IEC TR 27016:2014 (ISO 27016) Information technology - Security techniques - Information security management - Organisational economics	**ISO/IEC TR 27016:2014** 20.02.2014	ISO/IEC TR 27016:2014 provides guidelines on how an organisation can make decisions to protect information and understand the economic consequences of these decisions in the context of competing requirements for resources. ISO/IEC TR 27016:2014 is applicable to all types and sizes of organisations and provides information to enable economic decisions in information security management by top management who have responsibility for information security decisions.
15	ISO/IEC 27017:2015 (ISO 27017) Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services	**ISO/IEC 27017:2015** 30.11.2015	ISO/IEC 27017:2015 gives guidelines for information security controls applicable to the provision and use of cloud services by providing: - additional implementation guidance for relevant controls specified in ISO/IEC 27002; - additional controls with implementation guidance that specifically relate to cloud services. This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.

No.	Standard	Implemented	Note
16	**ISO/IEC 27018:2014** (ISO27018) Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	**ISO/IEC 27018:2019** 15.01.2019	This document establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. In particular, this document specifies guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which can be applicable within the context of the information security risk environment(s) of a provider of public cloud services. This document is applicable to all types and sizes of organisations, including public and private companies, government entities and not-for-profit organisations, which provide information processing services as PII processors via cloud computing under contract to other organisations. The guidelines in this document can also be relevant to organisations acting as PII controllers. However, PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors. This document is not intended to cover such additional obligations.
17	**ISO/IEC TR 27019:2013** (ISO 27019) Information technology - Security techniques - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry	**MEST EN ISO/IEC 27019:2020** 18.12.2020 **ISO/IEC 27019:2017** 01.11.2017	ISO/IEC 27019:2017 provides guidance based on ISO/IEC 27002:2013 applied to process control systems used by the energy utility industry for controlling and monitoring the production or generation, transmission, storage and distribution of electric power, gas, oil and heat, and for the control of associated supporting processes. This includes in particular the following: - central and distributed process control, monitoring and automation technology as well as information systems used for their operation, such as programming and parameterisation devices; - digital controllers and automation components such as control and field devices or Programmable Logic Controllers (PLCs), including digital sensor and actuator elements; - all further supporting information systems used in the process control domain, e.g. for supplementary data visualisation tasks and for controlling, monitoring, data archiving, historian logging, reporting and documentation purposes; - communication technology used in the process control domain, e.g. networks, telemetry, telecontrol applications and remote control technology; - Advanced Metering Infrastructure (AMI) components, e.g. smart meters; - measurement devices, e.g. for emission values;

No.	Standard	Implemented	Note
			- digital protection and safety systems, e.g. protection relays, safety PLCs, emergency governor mechanisms; - energy management systems, e.g. of Distributed Energy Resources (DER), electric charging infrastructures, in private households, residential buildings or industrial customer installations; - distributed components of smart grid environments, e.g. in energy grids, in private households, residential buildings or industrial customer installations; - all software, firmware and applications installed on above-mentioned systems, e.g. DMS (Distribution Management System) applications or OMS (Outage Management System); - any premises housing the above-mentioned equipment and systems; - remote maintenance systems for above-mentioned systems. ISO/IEC 27019:2017 does not apply to the process control domain of nuclear facilities. This domain is covered by IEC 62645. ISO/IEC 27019:2017 also includes a requirement to adapt the risk assessment and treatment processes described in ISO/IEC 27001:2013 to the energy utility industry-sector specific guidance provided in this document.
18	**ISO/IEC 27023:2015** (ISO 27023) Information technology - Security techniques - Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002	**ISO/IEC TR 27023:2015** 02.07.2015	ISO/IEC TR 27023:2015 is to show the corresponding relationship between the revised versions of ISO/IEC 27001 and ISO/IEC 27002. ISO/IEC TR 27023:2015 will be useful to all users migrating from the 2005 to the 2013 versions of ISO/IEC 27001 and ISO/IEC 27002.

No.	Standard	Implemented	Note
19	ISO/IEC 27032:2012 (ISO 27032) Information technology - Security techniques - Guidelines for cybersecurity	**ISO/IEC 27032:2012** 16.07.2012	ISO/IEC 27032:2012 provides guidance for improving the state of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular: information security, network security, internet security, and critical information infrastructure protection (CIIP). It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides: an overview of Cybersecurity, an explanation of the relationship between Cybersecurity and other types of security, a definition of stakeholders and a description of their roles in Cybersecurity, guidance for addressing common Cybersecurity issues, and a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.
20	ISO/IEC 27035-1:2016 (ISO 27035-1) Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management	**ISO/IEC 27035-1:2016** 28.10.2016	ISO/IEC 27035-1:2016 is the foundation of this multipart International Standard. It presents basic concepts and phases of information security incident management and combines these concepts with principles in a structured approach to detecting, reporting, assessing, and responding to incidents, and applying lessons learnt. The principles given in ISO/IEC 27035-1:2016 are generic and intended to be applicable to all organisations, regardless of type, size or nature. Organisations can adjust the guidance given in ISO/IEC 27035-1:2016 according to their type, size and nature of business in relation to the information security risk situation. It is also applicable to external organisations providing information security incident management services.
21	ISO/IEC 27036-1:2014 (ISO 27036-1) Information technology - Security techniques - Information security for supplier relationships - Part 1: Overview and concepts	**ISO/IEC 27036-1:2021** 09.09.2021	This document is an introductory part of ISO/IEC 27036. It provides an overview of the guidance intended to assist organisations in securing their information and information systems within the context of supplier relationships. It also introduces concepts that are described in detail in the other parts of ISO/IEC 27036. This document addresses perspectives of both acquirers and suppliers.

No.	Standard	Implemented	Note
22	ISO/IEC 27036-2:2014 (ISO 27036-2) Information technology - Security techniques - Information security for supplier relationships - Part 2: Requirements	**ISO/IEC 27036-2:2014** 25.07.2014	ISO/IEC 27036-2:2014 specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving supplier and acquirer relationships. These requirements cover any procurement and supply of products and services, such as manufacturing or assembly, business process procurement, software and hardware components, knowledge process procurement, Build-Operate-Transfer and cloud computing services. These requirements are intended to be applicable to all organisations, regardless of type, size and nature. To meet these requirements, an organisation should have already internally implemented a number of foundational processes, or be actively planning to do so. These processes include, but are not limited to, the following: governance, business management, risk management, operational and human resources management, and information security.
23	ISO/IEC 27036-3:2013 (ISO 27036-3) Information technology - Security techniques - Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security	**ISO/IEC 27036-3:2013** 08.11.2013	ISO/IEC 27036-3:2013 provides product and service acquirers and suppliers in the information and communication technology (ICT) supply chain with guidance on: gaining visibility into and managing the information security risks caused by physically dispersed and multi-layered ICT supply chains; responding to risks stemming from the global ICT supply chain to ICT products and services that can have an information security impact on the organisations using these products and services. These risks can be related to organisational as well as technical aspects (e.g. insertion of malicious code or presence of the counterfeit information technology (IT) products); integrating information security processes and practices into the system and software lifecycle processes, described in ISO/IEC 15288 and ISO/IEC 12207, while supporting information security controls, described in ISO/IEC 27002. ISO/IEC 27036-3:2013 does not include business continuity management/resiliency issues involved with the ICT supply chain. ISO/IEC 27031 addresses business continuity.

No.	Standard	Implemented	Note
24	**ISO/IEC 27038:2014** (ISO 27038) Information technology - Security techniques - Specification for digital redaction	**MEST EN ISO/IEC 27038:2017** 15.12.2017 **ISO/IEC 27038:2014** 13.03.2014.	ISO/IEC 27038:2014 specifies characteristics of techniques for performing digital redaction on digital documents. It also specifies requirements for software redaction tools and methods of testing that digital redaction has been securely completed. ISO/IEC 27038:2014 does not include the redaction of information from databases.
25	**ISO/IEC 27039:2015** (ISO 27039) Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems (IDPS)	**ISO/IEC 27039:2015** 11.02.2015	ISO/IEC 27039:2015 provides guidelines to assist organisations in preparing to deploy intrusion detection and prevention systems (IDPS). In particular, it addresses the selection, deployment, and operations of IDPS. It also provides background information from which these guidelines are derived.
26	**ISO/IEC 27040:2015** (ISO 27040) Information technology - Security techniques - Storage security	**MEST EN ISO/IEC 27040:2017** 15.12.2017 **ISO/IEC 27040:2015** 05.01.2015	ISO/IEC 27040:2015 provides detailed technical guidance on how organisations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to planning, design, documentation, and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, security of management activities related to the devices and media, security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use. Storage security is relevant to anyone involved in owning, operating, or using data storage devices, media, and networks. This includes senior managers, acquirers of storage product and service, and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information security or storage security, storage operation, or who are responsible for an organisation's overall security programme and security policy development. It is also relevant to anyone involved in planning, design, and implementation of the architectural aspects of storage network security. ISO/IEC 27040:2015 provides an overview of storage security concepts and related definitions. It includes guidance on the threat, design, and control aspects associated with typical storage scenarios and storage technology areas. In addition, it provides references to other International Standards and technical reports that address existing practices and techniques that can be applied to storage security.

No.	Standard	Implemented	Note
27	**ISO/IEC 27041:2015** (ISO 27041) Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative methods.	**ISO/IEC 27041:2015** 19.06.2015	ISO/IEC 27041:2015 provides guidance on mechanisms for ensuring that methods and processes used in the investigation of information security incidents are "fit for purpose". It encapsulates best practice on defining requirements, describing methods, and providing evidence that implementations of methods can be shown to satisfy requirements. It includes consideration of how vendor and third-party testing can be used to assist this assurance process. This document aims to - provide guidance on the capture and analysis of functional and non-functional requirements relating to an Information Security (IS) incident investigation, - give guidance on the use of validation as a means of assuring suitability of processes involved in the investigation, - provide guidance on assessing the levels of validation required and the evidence required from a validation exercise, - give guidance on how external testing and documentation can be incorporated in the validation process.
28	**ISO/IEC 27042:2015** (ISO 27042) Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence	**MEST EN ISO/IEC 27042:2017** 15.12.2017 **ISO/IEC 27042:2015** 19.06.2015	ISO/IEC 27042:2015 provides guidance on the analysis and interpretation of digital evidence in a manner which addresses issues of continuity, validity, reproducibility, and repeatability. It encapsulates best practice for selection, design, and implementation of analytical processes and recording sufficient information to allow such processes to be subjected to independent scrutiny when required. It provides guidance on appropriate mechanisms for demonstrating proficiency and competence of the investigative team. Analysis and interpretation of digital evidence can be a complex process. In some circumstances, there can be several methods which could be applied and members of the investigative team will be required to justify their selection of a particular process and show how it is equivalent to another process used by other investigators. In other circumstances, investigators may have to devise new methods for examining digital evidence which has not previously been considered and should be able to show that the method produced is "fit for purpose". Application of a particular method can influence the interpretation of digital evidence processed by that method. The available digital evidence can influence the selection of methods for further analysis of digital evidence which has already been acquired. ISO/IEC 27042:2015 provides a common framework for analytical and interpretational elements of information systems security incident handling, which can be used to assist in the implementation of new methods and provide a minimum common standard for digital evidence produced from such activities.

No.	Standard	Implemented	Note
29	**ISO/IEC 27043:2015** (ISO 27043) Information technology - Information technology - Security techniques - Incident investigation principles and processes	**MEST EN ISO/IEC 27043:2017** 15.12.2017 **ISO/IEC 27043:2015** 04.03.2015	ISO/IEC 27043:2015 provides guidelines based on idealised models for common incident investigation processes across various incident investigation scenarios involving digital evidence. This includes processes from pre-incident preparation through investigation closure, as well as any general advice and caveats on such processes. The guidelines describe processes and principles applicable to various kinds of investigations, including, but not limited to, unauthorised access, data corruption, system crashes, or corporate breaches of information security, as well as any other digital investigation. In summary, this International Standard provides a general overview of all incident investigation principles and processes without prescribing particular details within each of the investigation principles and processes covered in this International Standard. Many other relevant International Standards, where referenced in this International Standard, provide more detailed content of specific investigation principles and processes.
30	**ISO 27799:2008** (ISO 27799) Health informatics - Information security management in health using ISO/IEC 27002	**MEST EN ISO 27799:2017** 22.06.2017 **ISO 27799:2016** 01.07.2016	ISO 27799:2016 gives guidelines for organisational information security standards and information security management practices including selection, implementation and management of controls taking into consideration the organisation's information security risk environment(s). It defines guidelines to support interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that International Standard. ISO 27799:2016 provides implementation guidance for the controls described in ISO/IEC 27002 and supplements them where necessary, so that they can be effectively used for managing health information security. By implementing ISO 27799:2016, healthcare organisations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organisation's circumstances and that will maintain the confidentiality, integrity and availability of personal health information in their care. It applies to health information in all its aspects, whatever form the information takes (words and numbers, sound recordings, drawings, video, and medical images), whatever means are used to store it (printing or writing on paper or storage electronically), and whatever means are used to transmit it (by hand, through fax, over computer networks, or by post), as the information is always appropriately protected.

No.	Standard	Implemented	Note
			ISO 27799:2016 and ISO/IEC 27002 taken together define what is required in terms of information security in healthcare, they do not define how these requirements are to be met. That is to say, to the fullest extent possible, ISO 27799:2016 is technology-neutral. Neutrality with respect to implementing technologies is an important feature. Security technology is still undergoing rapid development and the pace of that change is now measured in months rather than years. By contrast, while subject to periodic review, International Standards are expected on the whole to remain valid for years. Just as importantly, technological neutrality leaves vendors and service providers free to suggest new or developing technologies that meet the necessary requirements that ISO 27799:2016 describes. As noted in the introduction, familiarity with ISO/IEC 27002 is indispensable to an understanding of ISO 27799:2016. The following areas of information security are outside the scope of ISO 27799:2016: a) methodologies and statistical tests for effective anonymisation of personal health information; b) methodologies for pseudonymisation of personal health information (see Bibliography for a brief description of a Technical Specification that deals specifically with this topic); c) network quality of service and methods for measuring availability of networks used for health informatics; d) data quality (as distinct from data integrity).

No.	Standard	Implemented	Note
Network security standards			
1	**ISO/IEC 27033-1:2015** (ISO 27033-1) Information technology - Security techniques - Network security - Part 1: Overview and concepts	**ISO/IEC 27033-1:2015** 10.08.2015	ISO/IEC 27033-1:2015 provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security. (Network security applies to the security of devices, security of management activities related to the devices, applications/services, and end-users, in addition to security of the information being transferred across the communication links.) It is relevant to anyone involved in owning, operating or using a network. This includes senior managers and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information security and/or network security, network operation, or who are responsible for an organisation's overall security programme and security policy development. It is also relevant to anyone involved in the planning, design and implementation of the architectural aspects of network security. ISO/IEC 27033-1:2015 also includes the following: - provides guidance on how to identify and analyse network security risks and the definition of network security requirements based on that analysis, - provides an overview of the controls that support network technical security architectures and related technical controls, as well as those non-technical controls and technical controls that are applicable not just to networks, - introduces how to achieve good quality network technical security architectures, and the risk, design and control aspects associated with typical network scenarios and network "technology" areas (which are dealt with in detail in subsequent parts of ISO/IEC 27033), and briefly addresses the issues associated with implementing and operating network security controls, and the on-going monitoring and reviewing of their implementation. Overall, it provides an overview of this International Standard and a roadmap to all other parts.

No.	Standard	Implemented	Note
2	**ISO/IEC 27033-2:2012** (ISO 27033-2) Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security	**ISO/IEC 27033-2:2012** 27.07.2012	ISO/IEC 27033-2:2012 gives guidelines for organisations to plan, design, implement and document network security.
3	**ISO/IEC 27033-3:2010** (ISO27033-3) Information security - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues	**ISO/IEC 27033-3:2010** 03.12.2010	ISO/IEC 27033-3:2010 describes the threats, design techniques and control issues associated with reference network scenarios. For each scenario, it provides detailed guidance on the security threats and the security design techniques and controls required to mitigate the associated risks. Where relevant, it includes references to ISO/IEC 27033-4 to ISO/IEC 27033-6 to avoid duplicating the content of those documents. The information in ISO/IEC 27033-3:2010 is for use when reviewing technical security architecture/design options and when selecting and documenting the preferred technical security architecture/design and related security controls, in accordance with ISO/IEC 27033-2. The particular information selected (together with information selected from ISO/IEC 27033-4 to ISO/IEC 27033-6) will depend on the characteristics of the network environment under review, i.e. the particular network scenario(s) and 'technology' topic(s) concerned. Overall, ISO/IEC 27033-3:2010 will aid considerably the comprehensive definition and implementation of security for any organisation's network environment.
4	**ISO/IEC 27033-4:2014** (ISO27033-4) Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways	**ISO/IEC 27033-4:2014** 21.02.2014	ISO/IEC 27033-4:2014 gives guidance for securing communications between networks using security gateways (firewall, application firewall, Intrusion Protection System, etc.) in accordance with a documented information security policy of the security gateways, including: - identifying and analysing network security threats associated with security gateways; - defining network security requirements for security gateways based on threat analysis; - using techniques for design and implementation to address the threats and control aspects associated with typical network scenarios; and - addressing issues associated with implementing, operating, monitoring and reviewing network security gateway controls.

No.	Standard	Implemented	Note
5	**ISO/IEC 27033-5:2013** (ISO 27033-5) Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)	**ISO/IEC 27033-5:2013** 29.07.2013	ISO/IEC 27033-5:2013 gives guidelines for the selection, implementation, and monitoring of technical controls necessary to provide network security using Virtual Private Network (VPN) connections to interconnect networks and connect remote users to networks.
6	**ISO/IEC 27034-1:2011** (ISO 27034-1) Information technology - Security techniques - Application security - Part 1: Overview and concepts	**ISO/IEC 27034-1:2011** 21.11.2011	ISO/IEC 27034 provides guidance to assist organisations in integrating security into the processes used for managing their applications. ISO/IEC 27034-1:2011 presents an overview of application security. It introduces definitions, concepts, principles and processes involved in application security. ISO/IEC 27034 is applicable to in-house developed applications, applications acquired from third parties, and where development or operation of the application is outsourced.
7	**ISO/IEC 27034-2:2015** (ISO 27034-2) Information technology - Security techniques - Application security - Part 2: Organisation normative framework for application security	**ISO/IEC 27034-2:2015** 28.07.2015	ISO/IEC 27034-2:2015 provides a detailed description of the Organisation Normative Framework and provides guidance to organisations for its implementation.

No.	Standard	Implemented	Note
Risk management standards			
1	**ISO/IEC 31010:2009** (ISO 31010) Risk management - Risk assessment techniques	**MEST EN IEC 31010:2020** 11.03.2020 **IEC 31010:2019** 17.06.2019	IEC 31010:2019 is published as a double logo standard with ISO and provides guidance on the selection and application of techniques for assessing risk in a wide range of situations. The techniques are used to assist in making decisions where there is uncertainty, to provide information about particular risks and as part of a process for managing risk. The document provides summaries of a range of techniques, with references to other documents where the techniques are described in more detail. This second edition cancels and replaces the first edition published in 2009. This edition constitutes a technical revision. This edition includes the following significant technical changes with respect to the previous edition: more detail is given on the process of planning, implementing, verifying and validating the use of the techniques; the number and range of application of the techniques has been increased; the concepts covered in ISO 31000 are no longer repeated in this standard.
2	**ISO 31000:2009** (ISO 31000) Risk management - Principles and guidelines	**MEST ISO 31000:2018** 29.05.2018 **ISO 31000:2018** 14.02.2018	ISO 31000:2018 provides guidelines on managing risk faced by organisations. The application of these guidelines can be customised to any organisation and its context. ISO 31000:2018 provides a common approach to managing any type of risk and is not industry or sector specific. ISO 31000:2018 can be used throughout the life of the organisation and can be applied to any activity, including decision-making at all levels.

No.	Standard	Implemented	Note
Business continuity and disaster recovery standards			
1	**ISO/IEC 27031:2011** (ISO 27031) Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity	**ISO/IEC 27031:2011** 01.03.2011	ISO/IEC 27031:2011 describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organisation's ICT readiness to ensure business continuity. It applies to any organisation (private, governmental, and non-governmental, irrespective of size) developing its ICT readiness for business continuity programme (IRBC), and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions. It also enables an organisation to measure performance parameters that correlate to its IRBC in a consistent and recognised manner. The scope of ISO/IEC 27031:2011 encompasses all events and incidents (including security related) that could have an impact on ICT infrastructure and systems. It includes and extends the practices of information security incident handling and management and ICT readiness planning and services.
2	**ISO/IEC 22301:2012** (ISO 22301) Societal security - Business continuity management systems - Requirements	**MEST EN ISO 22301:2020** 11.03.2020 **ISO 22301:2019** 30.10.2019	This document specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise. The requirements specified in this document are generic and intended to be applicable to all organisations, or parts thereof, regardless of type, size and nature of the organisation. The extent of application of these requirements depends on the organisation's operating environment and complexity. This document is applicable to all types and sizes of organisations that: a) implement, maintain and improve a BCMS; b) seek to ensure conformity with stated business continuity policy; c) need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption; d) seek to enhance their resilience through the effective application of the BCMS. This document can be used to assess an organisation's ability to meet its own business continuity needs and obligations.

No.	Standard	Implemented	Note
3	ISO 22300:2012 (ISO 22300) Societal security - Terminology	**MEST EN ISO 22300:2019** 28.06.2019 **ISO 22300:2021** 24.02.2021	This document defines terms used in security and resilience standards.
4	ISO 22313:2012 (ISO 22313) Societal security - Business continuity management systems - Guidance	**MEST EN ISO 22313:2020** 18.12.2020 **ISO 22313:2020** 20.02.2020	This document gives guidance and recommendations for applying the requirements of the business continuity management system (BCMS) given in ISO 22301. The guidance and recommendations are based on good international practice. This document is applicable to organisations that: a) implement, maintain and improve a BCMS; b) seek to ensure conformity with stated business continuity policy; c) need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption; d) seek to enhance their resilience through the effective application of the BCMS. The guidance and recommendations are applicable to all sizes and types of organisations, including large, medium and small organisations operating in industrial, commercial, public and not-for-profit sectors. The approach adopted depends on the organisation's operating environment and complexity.

No.	Standard	Implemented	Note
Quality management standards			
1	**ISO 9000:2015** (ISO 9000) Quality management systems - Fundamentals and vocabulary	**MEST EN ISO 9000:2016** 14.03.2016 **ISO 9000:2015** 22.09.2015	ISO 9000:2015 describes the fundamental concepts and principles of quality management which are universally applicable to the following: organisations seeking sustained success through the implementation of a quality management system; customers seeking confidence in an organisation's ability to consistently provide products and services conforming to their requirements; organisations seeking confidence in their supply chain that their product and service requirements will be met; organisations and interested parties seeking to improve communication through a common understanding of the vocabulary used in quality management; organisations performing conformity assessments against the requirements of ISO 9001; providers of training, assessment or advice in quality management; developers of related standards. ISO 9000:2015 specifies the terms and definitions that apply to all quality management and quality management system standards developed by ISO/TC 176.
2	**ISO 9001:2015** (ISO 9000) Quality management systems - Requirements	**MEST EN ISO 9001:2016** 03.06.2016 **ISO 9001:2015** 22.09.2015	ISO 9001:2015 specifies requirements for a quality management system when an organisation: a) needs to demonstrate its ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, and b) aims to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements. All the requirements of ISO 9001:2015 are generic and are intended to be applicable to any organisation, regardless of its type or size, or the products and services it provides.

No.	Standard	Implemented	Note
Software standards			
1	**ISO/IEC 19770-1:2012** (ISO 19770-1) Information technology - Software asset management - Part 1: Processes and tiered assessment of conformance	**ISO/IEC 19770-1:2017** 07.12.2017	ISO/IEC 19770-1:2017 specifies requirements for an IT asset management system within the context of the organisation. ISO/IEC 19770-1:2017 can be applied to all types of IT assets and by all types and sizes of organisations. NOTE 1 This document is intended to be used for managing IT assets in particular, but it can also be applied to other asset types. It can be suitable, in whole or in part, for managing embedded software and firmware, however its use for these purposes has not been determined. It is not intended for managing information assets per se, i.e. it is not intended for managing information as an asset independent of hardware and software assets. Certain types of data and information are covered, such as data and information about IT assets in scope, and depending on how the scope is defined, it can cover digital information content assets. See the Introduction for an explanation about IT assets. NOTE 2 This document does not specify financial, accounting, or technical requirements for managing specific IT asset types. NOTE 3 For the purposes of this document, the term “IT asset management system” is used to refer to a management system for IT asset management. ISO/IEC 19770-1:2017 is a discipline-specific extension of ISO 55001:2014, with changes, and is not a sector-specific application of that International Standard. ISO 55001:2014 is intended to be used for managing physical assets in particular, but it can also be applied to other asset types. This document specifies requirements for the management of IT assets which are additional to those specified in ISO 55001:2014. Conformance to this document does not imply conformance to ISO 55001:2014. ISO/IEC 19770-1:2017 can be used by internal and external parties to assess the organisation’s ability to meet the organisation’s own IT asset management requirements.

No.	Standard	Implemented	Note
2	ISO/IEC 19770-2:2015 (ISO 197701-2) Information technology - Software asset management - Part 2: Software identification tag	**ISO/IEC 19770-2:2015** 30.09.2015	ISO/IEC 19770-2:2015 establishes specifications for tagging software to optimise its identification and management. This part of ISO/IEC 19770 applies to the following. a) Tag producers: these organisations and/or tools create software identification (SWID) tags for use by others in the market. A tag producer may be part of the software creator organisation, the software licensor organisation, or be a third-party organisation. These organisations and/or tools can broadly be broken down into the following categories. Platform providers: entities responsible for the computer or hardware device and/or associated operating system, virtual environment, or application platform, on which software may be installed or run. Platform providers which support this part of ISO/IEC 19770 may additionally provide tag management capabilities at the level of the platform or operating system. Software providers: entities that create, license, or distribute software. For example, software creators, independent software developers, consultants, and repackagers of previously manufactured software. Software creators may also be in-house software developers. Tag tool providers: entities that provide tools to create software identification tags. For example, tools within development environments that generate software identification tags, or installation tools that may create tags on behalf of the installation process, and/or desktop management tools that may create tags for installed software that did not originally have a software identification tag. b) Tag consumers: these tools and/or organisations utilise information from SWID tags and are typically broken down into the following two major categories: software consumers: entities that purchase, install, and/or otherwise consume software; IT discovery and processing tool providers: entities that provide tools to collect, store, and process software identification tags. These tools may be targeted at a variety of different market segments, including software security, compliance, and logistics. ISO/IEC 19770-2:2015 does not prescribe Information Technology Asset Management (ITAM) or other IT-related processes required for reconciliation of software entitlements with software identification tags or other IT requirements. ISO/IEC 19770-2:2015 is not intended to conflict either with any organisation's policies, procedures or standards or with any domestic or international laws and regulations.

No.	Standard	Implemented	Note
Corporate governance standards			
1	**ISO/IEC 38500:2015** (ISO 38500) Information technology - Governance of IT for the organisation	**ISO/IEC 38500:2015** 11.02.2015	ISO/IEC 38500:2015 provides guiding principles for members of governing bodies of organisations (which can comprise owners, directors, partners, executive managers, or similar) on the effective, efficient, and acceptable use of information technology (IT) within their organisations. It also provides guidance to those advising, informing, or assisting governing bodies. They include the following: executive managers; members of groups monitoring the resources within the organisation; external business or technical specialists, such as legal or accounting specialists, retail or industrial associations, or professional bodies; internal and external service providers (including consultants); auditors. ISO/IEC 38500:2015 applies to the governance of the organisation's current and future use of IT including management processes and decisions related to the current and future use of IT. These processes can be controlled by IT specialists within the organisation, external service providers, or business units within the organisation. ISO/IEC 38500:2015 defines the governance of IT as a subset or domain of organisational governance, or in the case of a corporation, corporate governance. ISO/IEC 38500:2015 is applicable to all organisations, including public and private companies, government entities, and not-for-profit organisations. ISO/IEC 38500:2015 is applicable to organisations of all sizes from the smallest to the largest, regardless of the extent of their use of IT. The purpose of ISO/IEC 38500:20015 is to promote effective, efficient, and acceptable use of IT in all organisations by: assuring stakeholders that, if the principles and practices proposed by the standard are followed, they can have confidence in the organisation's governance of IT, informing and guiding governing bodies in governing the use of IT in their organisation, and establishing a vocabulary for the governance of IT.

No.	Standard	Implemented	Note
Certification and Assessment Standards			
1		**MEST EN ISO/IEC 15408-2:2020** 18.12.2020 **ISO/IEC 15408-1:2009** 03.12.2009	ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products. It provides an overview of all parts of ISO/IEC 15408. It describes the various parts of ISO/IEC 15408; defines the terms and abbreviations to be used in all parts ISO/IEC 15408; establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given. It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations. The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation and evaluation results are described. ISO/IEC 15408-1:2009 gives guidelines for the specification of Security Targets (ST) and provides a description of the organisation of components throughout the model. General information about the evaluation methodology is given in ISO/IEC 18045 and the scope of evaluation schemes is provided.
		MEST EN ISO/IEC 15408-3:2020 18.12.2020 **ISO/IEC 15408-3:2008** 19.08.2008	ISO/IEC 15408-3:2008 defines the assurance requirements of the evaluation criteria. It includes the evaluation assurance levels that define a scale for measuring assurance for component targets of evaluation (TOEs), the composed assurance packages that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of protection profiles and security targets. ISO/IEC 15408-3:2008 defines the content and presentation of the assurance requirements in the form of assurance classes, families and components and provides guidance on the organisation of new assurance requirements. The assurance components within the assurance families are presented in a hierarchical order.

No.	Standard	Implemented	Note
2	**ISO/IEC 29169:2016** Information technology - Process assessment - Application of conformity assessment methodology to the assessment to process quality characteristics and organisational maturity	**ISO/IEC 29169:2016** 06.04.2016	ISO/IEC 29169:2016 aims to define the application of a conformity assessment methodology, based on the existing published ISO/IEC standards and guides, to the process assessment of process quality characteristics and organisational process maturity, performed in accordance with the requirements of the ISO/IEC 33001 to ISO/IEC 33099 family of process assessment standards, Conformity assessment, also known as compliance assessment, is any activity to determine, directly or indirectly, that a process, product, or service meets relevant standards and fulfils relevant requirements. The subject of conformity assessment activities may include testing, inspection or certification. Conformity assessment in this International Standard can be performed by various types of bodies that meet the requirements of ISO/IEC 17020. The term "inspection" as used in ISO/IEC 17020 is synonymous with the term "process assessment" as defined in ISO/IEC 33001 and used throughout the ISO/IEC 33001 to ISO/IEC 33099 family of standards. While a process assessment may be performed solely according to the ISO/IEC 33002 requirements for performing an assessment, performing a process assessment in the context of conformity assessment according to a conformity assessment scheme brings with it additional requirements. Conformity assessment involves a functional approach consisting of a number of stages: selection, determination, review and attestation, plus surveillance when there is a need to provide continuing assurance of conformity.
3	**ISO/IEC TR 33018:2019** Information technology - Process assessment - Guidance for assessor competency	**ISO/IEC TR 33018:2019** 11.07.2019	This document provides general and specific guidance for the competency of assessors performing assessments in accordance with the ISO/IEC 330xx family of standards.

How the Montenegro eID scheme meets the interoperability and minimum technical and operational security requirements of Commission Implementing Regulation (EU) 2015/1501?

A: Law on Electronic Identification and Electronic Signature regulates the area of electronic identification in art. 61-67. Provisions of Article 10, paragraph 3, Art. 22, 36, Article 40, paragraphs 2 and 6, Article 43, Article 45, paragraph 4, Article 58, paragraphs 4 and 6, and Art. 62 to 67 of this Law will apply from the date of Montenegro's accession to the European Union.

Article	Requirement	Description
1	Mapping of national assurance levels The mapping of national assurance levels of the notified electronic identification schemes shall follow the requirements laid down in Implementing Regulation (EU) 2015/1502. The results of the mapping shall be notified to the Commission using the notification template laid down in Commission Implementing Decision (EU) 2015/1505	Economy level: MUP (Ministry of Internal Affairs) Crnogorski telekom
2	Nodes 1. A node in one Member State shall be able to connect with nodes of other Member States. 2. The nodes shall be able to distinguish between public sector bodies and other relying parties through technical means. 3. A Member State implementation of the technical requirements set out in this Regulation shall not impose disproportionate technical requirements and costs on other Member States in order for them to interoperate with the implementation adopted by the first Member State.	Article 62 The Ministry cooperates with the Member States of the European Union regarding: 1) interoperability of electronic identification systems that are entered in the register of electronic identification systems; 2) security of the electronic identification system. Cooperation from paragraph 1 of this Article implies: 1) exchange of information, experience and good practice in relation to electronic identification systems, in particular in relation to technical requirements relating to interoperability and security levels relating to electronic identification systems;

Article	Requirement	Description
		2) exchange of information, experience and good practice regarding security levels relating to electronic identification; 3) exchange of information on the evaluation of conformity of the electronic identification system.
3	Data privacy and confidentiality 1. Protection of privacy and confidentiality of the data exchanged and the maintenance of data integrity between the nodes shall be ensured by using best available technical solutions and protection practices. 2. The nodes shall not store any personal data, except for the purpose set out in Article 9(3)	Ministry adopted ***Regulations on technical and operational requirements relating to the node - the place of connection of the electronic identification system and the process establishing a framework for interoperability of electronic identification***.
4	Data integrity and authenticity for the communication Communication between the nodes shall ensure data integrity and authenticity to make certain that all requests and responses are authentic and have not been tampered with. For this purpose, nodes shall use solutions which have been successfully employed in cross-border/boundary operational use.	Ministry adopted ***Regulations on technical and operational requirements relating to the node - the place of connection of the electronic identification system and the process establishing a framework for interoperability of electronic identification***.
5	Message format for the communication The nodes shall use for syntax common message formats based on standards that have already been deployed more than once between Member States and proven to work in an operational environment. The syntax shall allow: (a) proper processing of the minimum set of person identification data uniquely representing a natural or legal person; (b) proper processing of the assurance level of the electronic identification means; (c) distinction between public sector bodies and other relying parties; d) flexibility to meet the needs of additional attributes relating to identification	Article 62 The Ministry cooperates with the Member States of the European Union regarding: 1) interoperability of electronic identification systems that are entered in the register of electronic identification systems; 2) security of the electronic identification system. Cooperation from paragraph 1 of this Article implies: 1) exchange of information, experience and good practice in relation to electronic identification systems, in particular in relation to technical requirements relating to interoperability and security levels relating to electronic identification systems; 2) exchange of information, experience and good practice regarding security levels relating to electronic identification; 3) exchange of information on evaluation of the conformity of the electronic identification system.

Article	Requirement	Description
6	Management of security information and metadata 1. The node operator shall communicate the metadata of the node management in a standardised machine processable manner and in a secure and trustworthy way. 2. At least the parameters relevant to security shall be retrieved automatically. 3. The node operator shall store data which, in the event of an incident, enable reconstruction of the sequence of the message exchange for establishing the place and the nature of the incident. The data shall be stored for a period of time in accordance with domestic requirements and, as a minimum, shall consist of the following elements: (a) node's identification; (b) message identification; (c) message data and time	Ministry adopted ***Regulations on technical and operational requirements relating to the node - the place of connection of the electronic identification system and the process establishing a framework for interoperability of electronic identification***.
7	Information assurance and security standards 1. Node operators of nodes providing authentication shall prove that, in respect of the nodes participating in the interoperability framework, the node fulfils the requirements of standard ISO/IEC 27001 by certification, or by equivalent methods of assessment, or by complying with domestic legislation. 2. Node operators shall deploy security critical updates without undue delay.	Ministry adopted ***Regulations on technical and operational requirements relating to the node - the place of connection of the electronic identification system and the process establishing a framework for interoperability of electronic identification***.
8	Person identification data 1. A minimum set of person identification data uniquely representing a natural or a legal person shall meet the requirements set out in the Annex when used in a cross-border/boundary context. 2. A minimum data set for a natural person representing a legal person shall contain the combination of the attributes listed in the Annex for natural persons and legal persons when used in a cross-border/boundary context. 3. Data shall be transmitted based on original characters and, where appropriate, also transliterated into Latin characters	Ministry adopted ***Regulations on technical and operational requirements relating to the node - the place of connection of the electronic identification system and the process establishing a framework for interoperability of electronic identification***.

Which of the following technical standards, reports, and specifications recommended by ENISA were implemented in Montenegro in relation to trust services?

No.	Standard	Implemented	Note
1	**ETSI EN 319 102-1:** "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation"	Rulebook on measures and activities for the protection of certificates for electronic signature and electronic seal	
2	**ETSI TS 119 102-1 (V1.2.1):** "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation"	**MEST ETSI TS 119 102-1 V1.2.1:2019** 15.03.2019	The present document specifies procedures for: • the creation of AdES digital signatures (specified in ETSI EN 319 122-1 [i.2], ETSI EN 319 132-1 [i.4], ETSI EN 319 142-1 [i.6] respectively); • establishing whether an AdES digital signature is technically valid; whenever the AdES digital signature is based on public key cryptography and supported by public key certificates. To improve readability of the present document, AdES digital signatures are meant when the term signature is being used.
3	**ETSI TS 119 102-2:** "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report"	**MEST ETSI TS 119 102-2 V1.1.1:2019** 15.03.2019.	The present document specifies a general structure and an XML format for reporting the validation of AdES digital signatures (specified in ETSI EN 319 122-1 [i.1], ETSI EN 319 132-1 [4], ETSI EN 319 142-1 [i.3] respectively). The present document is aligned with the requirements specified in ETSI TS 119 102-1 [1].

No.	Standard	Implemented	Note
4	**ETSI EN 319 122 series:** Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: "Building blocks and CAdES baseline signatures" Part 2: "Extended CAdES signatures"	**MEST ETSI TS 119 122-3 V1.1.1:2018** 20.12.2018 Rulebook on measures and activities for the protection of certificates for electronic signature and electronic seal	The present document provides mechanism to incorporate evidence records in ASN.1 format within a CAdES signature as outlined in ETSI EN 319 122-1 [4], Annex B. It specifies the attributes to be used and profiles of the ERS standard (IETF RFC 4998 [2]) to provide clear rules how to incorporate ERS within a CAdES signature or a legacy CAdES signature.
5	**ETSI EN 319 132 series:** Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: "Building blocks and XAdES baseline signatures" Part 2: "Extended XAdES signatures"	Rulebook on measures and activities for the protection of certificates for electronic signature and electronic seal	
6	**ETSI EN 319 142 series:** Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: "Building blocks and PAdES baseline signatures" Part 2: "Additional PAdES signatures profiles"	**MEST EN 319 142-1 V1.1.1:2018** 20.12.2018. **ETSI EN 319 142-1 V1.1.1:2016** Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures	The present document specifies a type of PDF digital signatures, as specified in ISO 32000-1 [1], based on time-stamps. It specifies a format for PAdES digital signatures using a Document Time-stamp - as defined in ETSI EN 319 142-1 [2] - as a digital signature intended to specifically prove the integrity and existence of a PDF document as defined in ISO 32000-1 [1], rather than proving any form of authentication or proof of origin.

No.	Standard	Implemented	Note
7	**ETSI TS 119 172 series:** Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: "Building blocks and table of contents for human readable signature policy documents" Part 2: "XML Format for signature policies" Part 3: "ASN.1 Format for signature policies" Part 4: "Signature validation `policy for European qualified electronic signatures/seals using trusted lists"	**MEST ETSI TS 119 172-1 V1.1.1:2019** 15.03.2019 Rulebook on measures and activities for the protection of certificates for electronic signature and electronic seal	The present document defines the building blocks of signature policy and specifies a table of contents for human readable signature policy documents.
8	**ETSI TS 119 312:** "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"	**MEST ETSI TS 119 312 V1.2.1:2019** 15.03.2019 Rulebook on closer conditions to be met by a qualified provider of electronic trust services	
9	**ETSI EN 319 401 (v2.2.1):** "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"	Rulebook on closer conditions to be met by a qualified provider of electronic trust services Rulebook on measures and activities for the protection of certificates for electronic signature and electronic seal	

No.	Standard	Implemented	Note
10	**ETSI EN 319 411-1 (v1.2.2):** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements"	Rulebook on closer conditions to be met by a qualified provider of electronic trust services Rulebook on measures and activities for the protection of certificates for electronic signature and electronic seal	
11	**ETSI EN 319 411-2 (v1.1.1):** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates"	Rulebook on closer conditions to be met by a qualified provider of electronic trust services Rulebook on measures and activities for the protection of certificates for electronic signature and electronic seal	
12	**ETSI EN 319 412-2 (v2.2.2):** "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons"	Rulebook on measures and activities for the protection of certificates for electronic signature and electronic seal	
13	**ETSI EN 319 412-3:** "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons"	Rulebook on measures and activities for the protection of certificates for electronic signature and electronic seal	

No.	Standard	Implemented	Note
14	**ETSI EN 319 412-4:** "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates"	Rulebook on measures and activities for the protection of certificates for electronic signature and electronic seal	
15	**ETSI EN 319 412-5:** "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QcStatements"	Rulebook on measures and activities for the protection of certificates for electronic signature and electronic seal	
16	**ETSI EN 319 421 (v1.1.1):** "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"	Rulebook on closer conditions to be met by a qualified provider of electronic trust services Rulebook on measures and activities for the protection of certificates for electronic signature and electronic seal	
17	**ETSI EN 319 422 (v1.1.1):** "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles"	Rulebook on measures and activities for the protection of certificates for electronic signature and electronic seal	
18	**ETSI TS 119 441 (v1.1.1):** "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services"	**MEST ETSI TS 119 441 V1.1.1:2019** 15.03.2019.	The present document, based on the general policy requirements specified in ETSI EN 319 401 [2], specifies policy and security requirements for signature validation services operated by a TSP.

No.	Standard	Implemented	Note
19	**EN 301 549:** "Accessibility requirements for ICT products and services"	**MEST EN 301 549 V2.1.2:2019**	

Appendix II - Standards to be adopted

	List of CEN Standards to be adopted
1	**CEN TR 419 210:** "Applicability of CEN Standards to Qualified Electronic Seal Creation Device under the EU Regulation N°910/2014 (eIDAS)"
2	**CEN EN 419 221-5:** "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic Module for Trust Services"
3	**CEN EN 419 231:** "Protection profile for trustworthy systems supporting time stamping"
4	**CEN EN 419 241-1**: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements"
5	**CEN EN 419 241-2:** "Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing"
	List of ETSI standards to be adopted
1	**ETSI TR 119 000:** "Electronic Signatures and Infrastructures (ESI); The framework for standardisation of signatures: overview"
2	**ETSI TS 119 403-3:** "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers"
3	**ETSI TS 119 442:** "Electronic Signatures and Infrastructures (ESI); Protocol profiles for trust service providers providing AdES digital signature validation services"
4	**ETSI TS 119 495:** "Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366"
5	**ETSI TS 119 511:** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques"
6	**ETSI TS 119 512:** "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services"
7	**ETSI EN 319 521 (v1.1.1):** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers"

8	**ETSI EN 319 522 series:** Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; **Part 1 (v1.1.1):** "Framework and Architecture" **Part 2:** "Semantic contents" **Part 3:** "Formats" **Part 4:** "Bindings: **Sub-part 1:** "Message delivery bindings" **Sub-part 2:** "Evidence and identification bindings" **Sub-part 3:** "Capability/requirements bindings"
9	**ETSI TS 119 524** (all parts): "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services"
10	**ETSI EN 319 531 (v1.1.1):** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers"
11	**ETSI EN 319 532** series: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; **Part 1 (v1.1.1):** "Framework and Architecture" **Part 2:** "Semantic contents" **Part 3:** "Formats" **Part 4:** "Interoperability profiles"
12	**ETSI TS 119 534** (all parts): "Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Registered Electronic Mail Services"
13	**ETSI TS 119 612:** "Electronic Signatures and Infrastructures (ESI); Trusted Lists"
14	**ETSI TS 119 615:** "Electronic Signatures and Infrastructures (ESI); Trusted Lists; Procedures for using and interpreting European Union Member States national trusted lists"
15	**ETSI TR 103 684:** "Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services"
16	**ETSI TS 119 431-1 (v1.1.1):** "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev"

RegionalCooperationCouncil

Trg BiH 1/V, Sarajevo
Bosnia and Herzegovina

Fax: +387 33 561 701
Phone: +387 33 561 700

mail: rcc@rcc.int
website: www.rcc.int

@rccint

regionalcooperationcouncil_rcc

RegionalCooperationCouncil

RCCSec

Regional Cooperation Council

rcc.int